# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-261747
(43)Date of publication of application : 13.09.2002

(51)Int.Cl. H04L 9/08
G06F 15/00

(21)Application number : 2001-076918
(22)Date of filing : 16.03.2001

(71)Applicant : SONY CORP
(72)Inventor : KAMIYA SHIGEKI
YAMASHITA MASAMI

(30)Priority
Priority number : 2000403472 Priority date : 28.12.2000 Priority country : JP

## (54) DATA DISTRIBUTION METHOD AND DISTRIBUTION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To make requirements of the difficulty of unauthorized operation and reduction of the running cost compatible.
SOLUTION: When a decoding server permits an encryption process to be cancelled, the system scrambles digital data which decoding process is cancelled, using a scramble key generated in the decrypting server, and thus scrambled digital data are given to an output unit, thereby preventing any unauthorized operation on associated transmission paths, even if the decoding server is separated from the output unit.

LEGAL STATUS
[Date of request for examination] 16.03.2001
[Date of sending the examiner's decision of rejection] 19.10.2004
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

---

CLAIMS

---

[Claim(s)]

[Claim 1] The upstream system which carries out multi-point distribution of the digital data with which cipher processing was performed to the specific person, Are the distribution approach of the digital data performed between the downstream systems of which cipher processing performed to the digital data which received distribution is canceled, and an upstream system puts under the control. The processing which enciphers digital data by the corresponding cryptographic key, and the processing which generates two or more key information on a proper based on the above-mentioned cryptographic key at each specific person who is a distribution place, The processing which distributes two or more generated key information using what is a distribution path different from digital data, and serves as another distribution path also in between key information, In the bottom of control of the decode server which the downstream system which performs processing which distributes the digital data with which cipher processing was performed, and receives distribution of the digital data concerned can open only in the procedure of normal The processing which restores the cryptographic key of digital data [ / based on two or more key information that distribution was received through two or more distribution paths ], The processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled, In the only output destination change of the digital data of which the processing which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, and cipher processing were canceled In the processing which decrypts the coding processing performed to the digital data concerned, and restores the former data of digital data, and the only output destination change of the restored digital data Perform processing which carries out scramble processing and outputs the former data of digital data using the scramble key generated by the above-mentioned processing, and it puts under control of the

output unit which can be opened only in the procedure of normal. The processing of which the scramble processing performed to the digital data inputted from the above-mentioned decode server is canceled with the scramble discharge key given from the above-mentioned decode server, The distribution approach of the digital data characterized by performing processing which outputs the digital data concerned with a predetermined output gestalt in the only output destination change of the digital data of which the scramble was canceled by the above-mentioned processing.
[Claim 2] The upstream system which carries out multi-point distribution of the digital data with which cipher processing was performed to the specific person, Are the distribution approach of the digital data performed between the downstream systems of which cipher processing performed to the digital data which received distribution is canceled, and an upstream system puts under the control. The processing which enciphers digital data by the corresponding cryptographic key, and the processing which generates the doubling key of the lot of a proper based on the above-mentioned cryptographic key at each specific person who is a distribution place, The processing which doubles and distributes a key or its generating information using the generated thing which is a distribution path different from digital data, and serves as another distribution path also in mutual, In the bottom of control of the decode server which the downstream system which performs processing which distributes the digital data with which cipher processing was performed, and receives distribution of the digital data concerned can open only in the procedure of normal The processing which restores the cryptographic key of digital data [ / based on the doubling key or its generating information on the lot which received distribution through two or more distribution paths ], The processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled, In the only output destination change of the digital data of which the processing which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, and cipher processing were canceled In the processing which decrypts the coding processing performed to the digital data concerned, and restores the former data of digital data, and the only output destination change of the restored digital data Perform processing which carries out scramble processing and outputs the former data of digital data using the scramble key generated by the above-mentioned processing, and it puts under control of the output unit which can be opened only in the procedure of normal. The processing of which the scramble processing performed to the digital data inputted from the above-mentioned decode server is canceled with the scramble discharge key given from the above-mentioned decode server, The distribution approach of the digital data characterized by performing processing which outputs the digital data concerned with a predetermined output gestalt in the only output destination change of the digital data of which the scramble was canceled by the above-mentioned processing.
[Claim 3] The upstream system which carries out multi-point distribution of the digital

data with which cipher processing was performed to the specific person, Are the distribution approach of the digital data performed between the downstream systems of which cipher processing performed to the digital data which received distribution is canceled, and an upstream system puts under the control. The processing which enciphers digital data by the corresponding cryptographic key, and the processing which generates the doubling key of the lot of a proper based on the above-mentioned cryptographic key at each specific person who is a distribution place, The generated processing which doubles and generates further two or more partial keys about a part of key or its generating information, The processing which distributes the remaining doubling keys which were not used for generation of two or more partial keys concerned, or the generating information and these partial key of those, or the generating information of those using what digital data is another distribution path and serves as another distribution path also in mutual, In the bottom of control of the decode server which the downstream system which performs processing which distributes the digital data with which cipher processing was performed, and receives distribution of the digital data concerned can open only in the procedure of normal Two or more partial keys which received distribution through two or more distribution paths, or the generating information of those, The processing which restores the doubling key which makes these and a group, or the cryptographic key of digital data [ / based on the generating information ], The processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled, In the only output destination change of the digital data of which the processing which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, and cipher processing were canceled In the processing which decrypts the coding processing performed to the digital data concerned, and restores the former data of digital data, and the only output destination change of the restored digital data Perform processing which carries out scramble processing and outputs the former data of digital data using the scramble key generated by the above-mentioned processing, and it puts under control of the output unit which can be opened only in the procedure of normal. The processing of which the scramble processing performed to the digital data inputted from the above-mentioned decode server is canceled with the scramble discharge key given from the above-mentioned decode server, The distribution approach of the digital data characterized by performing processing which outputs the digital data concerned with a predetermined output gestalt in the only output destination change of the digital data of which the scramble was canceled by the above-mentioned processing.

[Claim 4] The upstream system which carries out multi-point distribution of the digital data with which cipher processing was performed to the specific person, Are the distribution approach of the digital data performed between the downstream systems of which cipher processing performed to the digital data which received distribution is

canceled, and an upstream system puts under the control. It is a proper at the processing which enciphers digital data by the corresponding cryptographic key, and each specific person who is a distribution place. Or the processing which generates the 2nd cryptographic key of a proper in digital data, The processing the above 1st was generated by whose 2nd cryptographic key of the above and which doubles and enciphers a key or its generating information, The processing which distributes the 1st enciphered cryptographic key concerned, its generating information and 2nd cryptographic key of the above, or its generating information using what digital data is another distribution path and serves as another distribution path also in mutual, In the bottom of control of the decode server which the downstream system which performs processing which distributes the digital data with which cipher processing was performed, and receives distribution of the digital data concerned can open only in the procedure of normal The processing which cancels cipher processing performed to the 1st cryptographic key which received distribution, or its generating information based on the 2nd cryptographic key which received distribution through two or more distribution paths, or its generating information, and restores the 1st cryptographic key, The processing of which cipher processing performed to the digital data which corresponds using the 1st restored cryptographic key is canceled, In the only output destination change of the digital data of which the processing which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, and cipher processing were canceled In the processing which decrypts the coding processing performed to the digital data concerned, and restores the former data of digital data, and the only output destination change of the restored digital data Perform processing which carries out scramble processing and outputs the former data of digital data using the scramble key generated by the above-mentioned processing, and it puts under control of the output unit which can be opened only in the procedure of normal. The processing of which the scramble processing performed to the digital data inputted from the above-mentioned decode server is canceled with the scramble discharge key given from the above-mentioned decode server, The distribution approach of the digital data characterized by performing processing which outputs the digital data concerned with a predetermined output gestalt in the only output destination change of the digital data of which the scramble was canceled by the above-mentioned processing.

[Claim 5] The upstream system which carries out multi-point distribution of the digital data with which cipher processing was performed to the specific person, Are the distribution approach of the digital data performed between the downstream systems of which cipher processing performed to the digital data which received distribution is canceled, and an upstream system puts under the control. It is a proper at the processing which enciphers digital data by the 1st cryptographic key, and each specific person who is a distribution place. Or the processing which generates the 2nd cryptographic key of a proper in digital data, Digital data is another distribution path

about the doubling key or its generating information on the lot generated from the processing which generates the doubling key of a lot based on the 2nd cryptographic key of the above, the 1st cryptographic key enciphered by the 2nd cryptographic key, or its generating information and 2nd cryptographic key of the above. Processing distributed using what serves as another distribution path also in mutual, and processing which distributes the digital data with which cipher processing was performed are performed. In the bottom of control of the decode server which the downstream system which receives distribution of the digital data concerned can open only in the procedure of normal The 2nd cryptographic key is restored based on the doubling key or its generating information on the lot which received distribution through two or more distribution paths. The processing which cancels cipher processing performed to the 1st cryptographic key which received distribution, or its generating information, and restores the 1st cryptographic key, The processing of which cipher processing performed to the digital data which corresponds using the 1st restored cryptographic key is canceled, In the only output destination change of the digital data of which the processing which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, and cipher processing were canceled In the processing which decrypts the coding processing performed to the digital data concerned, and restores the former data of digital data, and the only output destination change of the restored digital data Perform processing which carries out scramble processing and outputs the former data of digital data using the scramble key generated in the above-mentioned processing, and it puts under control of the output unit which can be opened only in the procedure of normal. The processing of which the scramble processing performed to the digital data inputted from the above-mentioned decode server is canceled with the scramble discharge key given from the above-mentioned decode server, The distribution approach of the digital data characterized by performing processing which outputs the digital data concerned with a predetermined output gestalt in the only output destination change of the digital data of which the scramble was canceled by the above-mentioned processing.

[Claim 6] The decode server which performs predetermined signal processing in response to distribution of the digital data with which cipher processing was performed, It is a downstream system in an electronic distribution system equipped with the output unit which outputs contents with a predetermined output gestalt. The above-mentioned decode server The code discharge section which cancels cipher processing performed to the digital data in the distribution phase, The scramble control section which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, The decryption section which decrypts the coding processing which is the only output destination change of the digital data of which cipher processing was canceled in the above-mentioned code discharge section, and is performed to the digital data

concerned, and restores the former data of digital data, The scramble key which is the only output destination change of the restored digital data, and was generated in the above-mentioned scramble control section is used. It has the scramble processing section which carries out scramble processing and outputs the former data of digital data. The above-mentioned output unit The scramble discharge section which cancels the scramble processing performed to the digital data inputted from the above-mentioned receiving server with the scramble discharge key given from the above-mentioned receiving server, The downstream system in the electronic distribution system characterized by having the signal-processing section which is the only output destination change of the digital data of which the scramble was canceled in the above-mentioned scramble discharge section, and outputs the digital data concerned with a predetermined output gestalt.

[Claim 7] The code discharge section which is a decode server in the electronic distribution system which receives distribution of the digital data with which cipher processing was performed, and performs predetermined signal processing, and cancels cipher processing performed to the digital data in the distribution phase, The scramble control section which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, The decryption section which decrypts the coding processing which is the only output destination change of the digital data of which cipher processing was canceled in the above-mentioned code discharge section, and is performed to the digital data concerned, and restores the former data of digital data, The scramble key which is the only output destination change of the restored digital data, and was generated in the above-mentioned scramble control section is used. The decode server in the electronic distribution system characterized by having the scramble processing section which carries out scramble processing and outputs the former data of digital data.

[Claim 8] It is the circuit apparatus which realizes the function of the decode server in the electronic distribution system which performs predetermined signal processing in response to distribution of the digital data with which cipher processing was performed. The code discharge section which cancels cipher processing performed to the digital data in the distribution phase, The scramble control section which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, The decryption section which decrypts the coding processing which is the only output destination change of the digital data of which cipher processing was canceled in the above-mentioned code discharge section, and is performed to the digital data concerned, and restores the former data of digital data, The circuit apparatus characterized by having the scramble processing section which carries out scramble processing and outputs the former data of digital data using the scramble key which is the only output destination change of the restored digital data, and was generated in the above-mentioned scramble control

section.
[Claim 9] Code discharge processing in which cipher processing performed to digital contents in the distribution phase is canceled to a computer, The scramble control processing which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, As an only output destination change of the digital data of which cipher processing was canceled by the above-mentioned code discharge processing The decryption processing which decrypts the coding processing performed to the digital data concerned, and restores the former data of digital data, The scramble key generated in the above-mentioned scramble control processing as an only output destination change of the restored digital data is used. The record medium which is characterized by recording the program which performs scramble processing which carries out scramble processing and outputs the former data of digital data and in which computer reading is possible.
[Claim 10] The code discharge section which is a decode server in the electronic distribution system which receives distribution of the digital data with which cipher processing was performed, and performs predetermined signal processing, and cancels cipher processing performed to the digital data in the distribution phase, The decryption section which decrypts the coding processing which is the only output destination change of the digital data of which cipher processing was canceled in the above-mentioned code discharge section, and is performed to the digital data concerned, and restores the former data of digital data, The decode server in the electronic distribution system characterized by having the scramble processing section which is the only output destination change of the restored digital data, carries out scramble processing and outputs the former data of digital data using a scramble key.
[Claim 11] It is the circuit apparatus which realizes the function of the decode server in the electronic distribution system which performs predetermined signal processing in response to distribution of the digital data with which cipher processing was performed. The code discharge section which cancels cipher processing performed to the digital data in the distribution phase, The decryption section which decrypts the coding processing which is the only output destination change of the digital data of which cipher processing was canceled in the above-mentioned code discharge section, and is performed to the digital data concerned, and restores the former data of digital data, The circuit apparatus characterized by having the scramble processing section which is the only output destination change of the restored digital data, carries out scramble processing and outputs the former data of digital data using a predetermined scramble key.
[Claim 12] Code discharge processing in which cipher processing performed to the digital data in the distribution phase is canceled to a computer, As an only output destination change of the digital data of which cipher processing was canceled by the above-mentioned code discharge processing The decryption processing which

decrypts the coding processing performed to the digital data concerned, and restores the former data of digital data, The record medium which is characterized by recording the program which performs scramble processing which carries out scramble processing and outputs the former data of digital data as an only output destination change of the restored digital data using a predetermined scramble key and in which computer reading is possible.

[Claim 13] The decode server which carries out [ having the scramble control section which generates the discharge key for the partial decryption by the side of the output unit of the digital data enciphered with the scramble key and the scramble key concerned for partial encryption of the digital data outputted to an output unit, on condition that the playback conditions which are the decode server which cancels cipher processing performed to the digital data which received distribution, and are attached to digital data are fulfilled, and ] as the description.

[Claim 14] The circuit apparatus carry out having the scramble control section which generates in the discharge key for the partial decryption by the side of the output unit of the digital data enciphered with the scramble key and the scramble key concerned for partial encryption of the digital data outputted to an output unit from a decode server on condition that the playback conditions which are the circuit apparatus which realizes the function of the decode server which cancels cipher processing performed to the digital data which received distribution, and are attached to digital data are fulfilled as the description.

[Claim 15] The record medium possible in computer reading which carries out [ having recorded the program which performs the scramble control processing which generates the discharge key for the partial decryption by the side of the output unit of the digital data enciphered with the scramble key and the scramble key concerned for partial encryption of the digital data outputted to an output unit from a decode server, on condition that the playback conditions attached to the digital data which received distribution are fulfilled by the computer, and ] as the description.

[Claim 16] The output unit corresponding to the electronic distribution system carry out having the scramble discharge section which cancels the scramble processing which is an output unit corresponding to the electronic distribution system which outputs contents with a predetermined output gestalt, and is performed to the digital data inputted from a decode server with the scramble discharge key given from an above-mentioned decode server side, and the signal-processing section are the only output destination change of the digital data of which a scramble was canceled in the above-mentioned scramble discharge section, and output the digital data concerned at a predetermined output gestalt as the description.

[Claim 17] The circuit apparatus carry out having the scramble discharge section which cancels the scramble processing which is the circuit apparatus which can carry contents in the output unit corresponding to the electronic distribution system outputted with a predetermined output gestalt, and is performed to the digital data

inputted from the above-mentioned decode server with the scramble discharge key given from the above-mentioned decode server side as the description.
[Claim 18] The record medium which is characterized by recording the program which makes a computer perform scramble discharge processing in which a predetermined scramble discharge key cancels the scramble processing performed to the digital data inputted from a decode server and in which computer reading is possible.
[Claim 19] The decode server which performs predetermined signal processing in response to distribution of the digital data with which cipher processing was performed so that only a specific person could be reproduced, It is the signal-processing approach of the downstream system in an electronic distribution system equipped with the output unit which outputs contents with a predetermined output gestalt. The processing of which the above-mentioned decode server which can be opened only in the procedure of normal cancels cipher processing performed to the digital data in the distribution phase, In the only output destination change of the digital data of which cipher processing was canceled by the processing which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, and the above-mentioned processing In the processing which decrypts the coding processing performed to the digital data concerned, and restores the former data of digital data, and the only output destination change of the restored digital data Processing which carries out scramble processing and outputs the former data of digital data is performed using the scramble key generated by the above-mentioned processing. The processing of which the scramble processing to which the above-mentioned output unit which can be opened only in the procedure of normal is given to the digital data inputted from the above-mentioned decode server is canceled with the scramble discharge key given from the above-mentioned decode server, The signal-processing approach of the downstream system in the electronic distribution system characterized by performing processing which outputs the digital data concerned with a predetermined output gestalt in the only output destination change of the digital data of which the scramble was canceled by the above-mentioned processing.
[Claim 20] It is the signal-processing approach of the decode server in the electronic distribution system which performs predetermined signal processing in response to distribution of the digital data with which cipher processing was performed. The processing of which the above-mentioned decode server which can be opened only in the procedure of normal cancels cipher processing performed to the digital data in the distribution phase, In the only output destination change of the digital data of which the processing which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, and cipher processing were canceled In the processing which decrypts the coding processing performed to the digital data concerned, and restores the former data of digital data, and the only output destination change of the restored digital data The signal-

processing approach of the decode server in the electronic distribution system characterized by performing processing which carries out scramble processing and outputs the former data of digital data using the scramble key generated by the above-mentioned processing.

---

DETAILED DESCRIPTION

---

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the distribution approach of digital data, and a distribution system. Moreover, this invention relates to the component engineering required for the distribution approach of digital data, and distribution system implementation.
[0002]
[Description of the Prior Art] All digital data (alphabetic data (for example, a text, a notation, a graphic form), audio data (for example, voice, a musical piece), a video data (for example, a still picture, an animation), audio data, the complex data (for example, a movie, a program) of a video data, program data, digital data of database data and others) are going to be distributed through a network or a record medium with progress of a digital technique.
[0003] In addition, the digital data distributed may consist of two or more data files, if it may consist of a single data file. Moreover, there is a thing only including the information on single contents also about a data file, and there are some in which the information on two or more contents is included. Moreover, contents may be distributed by two or more digital data.
[0004]
[Problem(s) to be Solved by the Invention] On the other hand, since a perfect duplicate object can be created easily, if a malfeasance (for example, unjust decode playback, an unjust duplicate, sale through illegal channels) is performed, very serious damage will produce digital data. For this reason, making the structure which protects a contents provider (for example, a contents maker, the right person of distribution, a distribution entrepreneur) from a malfeasance is hurried. Since work takes huge costs and a huge help and immense damage arises by the malfeasance about the high contents (for example, movie) of asset value especially, making structure with a difficult malfeasance is called for.
[0005] However, the present condition is that the structure to which the both sides of a contents provider -- what has high defense capacity needs great plant-and-equipment investment, or some which there is comparatively little plant-and-

equipment investment, and end have a problem in defense capacity -- and a sink can be convinced is not established.
[0006] For example, when it continues keeping the resistance over a malfeasance high or the high output technique of repeatability appears more, it is desirable that a latest technology can be introduced suitably, but in order to take the configuration which prepares all functions required for a sink side in an output unit, according to the short thing of a technical life, the change of the output unit itself is needed in the business model by which the current proposal is made. However, in the business model on condition of a change in the short period of time of an output unit, an understanding by the side of a sink cannot be acquired. Moreover, as the result, replacement of the technique which obsoleted cannot progress easily, and there is evil in which the danger that digital data suits a malfeasance increases.
[0007] For this reason, a contents maker was not permitted offer of the high contents of asset value, the business model itself was not accepted in the sink side, but the problem of being unable to start operation of a system has arisen.
[0008] In consideration of the above technical problem, this application specification is proposed about the component engineering which realizes them in the system list to which the malfeasance applied the distribution approach that a high defense function can be maintained over a long period of time by the rational countervalue very difficult moreover, and the approach concerned until it reaches [ from the distribution phase of digital data ] a final output phase.
[0009]
[Means for Solving the Problem] The following means are proposed in order to solve this technical problem.
[0010] (1) Assume the distribution model which consists of each means below the distribution model assumed on this application specifications by the upstream system which performs processing mentioned later, and the downstream system.
[0011] What carries out multi-point distribution of the digital data with which cipher processing was performed is first assumed as an upstream system. For every digital data which is a candidate for distribution, although encryption processing here may be peculiar (namely, it enciphers by the cryptographic key of a proper for every digital data which is a candidate for distribution), it is not necessarily restricted to this. Of course, since the damage will arise only in the digital data unit concerned even if a malfeasance is performed if the thing of a proper is used for every digital data which is a candidate for distribution, there is an advantage which can minimize damage. However, when the case where the dependability of a system is high, and a simple distribution system are desired, cipher processing common about two or more digital data can be adopted. It depends on the request on business whether encryption processing [ which ] is adopted. Moreover, the distribution physically performed using a record medium besides the distribution of a mode performed through a transmission medium like distribution by distribution by broadcast or communication link is also

included in multi-point distribution here.
[0012] Moreover, an upstream system creates two or more key information on a proper to a distribution place or digital data with either of the approaches as shown below on the occasion of distribution of the cryptographic key used for encryption of digital data, and is a distribution path (the thing which differs in a medium physically, or thing which differs in a distribution time zone.) different from digital data about them. below the same. it is -- the distribution place which corresponds through what serves as another distribution path also in between key information, i.e., the method distributed to a downstream system, is adopted. That is, unless all other key information is stolen, it enables it to prevent generating of damage, even when the key information distributed through one of paths by distributing key information through two or more paths is stolen. In addition, not only the cryptographic key itself but the generating information (for example, random number) is sufficient as the key information distributed. Moreover, key information divided the cryptographic key and a key and a partial key are sufficient as it. Incidentally a common key system or a public key system is sufficient as a cipher system. Moreover, these compound methods may be used.
[0013] As an above-mentioned approach, the division pattern of a proper divides one cryptographic key for every distribution place, for example. Lot (not only a pair but three or more cases are included.) While generating the cryptographic key (the 2nd cryptographic key in a claim) from which a proper differs for every approach of generating partial key 2 distribution place While generating the cryptographic key (the 2nd cryptographic key in a claim) from which a proper differs every approach 3 which generates what enciphered the cryptographic key (the 1st cryptographic key in a claim) used for encryption of digital data by the cryptographic key concerned digital data There is the approach of generating what enciphered the cryptographic key (the 1st cryptographic key in a claim) used for encryption of digital data by the cryptographic key concerned.
[0014] In addition, it is not necessary to restrict to one the cryptographic key (the 2nd cryptographic key in a claim) from which a proper differs for every distribution place, and it may be used two or more. In this case, what is necessary is just to carry out encryption of the 1st cryptographic key twice or more (multiplex) by two or more 2nd cryptographic keys. Anyway, there is no difference at the point that the 1st cryptographic key is enciphered once or more by the 2nd cryptographic key. Moreover, the various encryption technique, such as performing cipher processing in multiplex, can be considered by combining a cryptographic key (for example, the cryptographic key which does not depend on the difference in a distribution place, but is used in common, a cryptographic key common to the cryptographic key of a proper, and two or more digital data for every digital data, other cryptographic keys) other than the 2nd cryptographic key.
[0015] The cryptographic key from which a proper differs for every division pattern of

a proper or distribution place for every distribution place here may be assigned each time for every digital data which is a candidate for distribution, if it may be assigned almost universally for every distribution person (if it may not be based on the difference in digital data but the comparatively same cryptographic key as a long period of time may be used). Of course, from a viewpoint of the cure against a malfeasance, the latter is desirable.

[0016] In addition, the approach of distributing physically using a record medium besides the approach of distributing electronically using a transmission network (network) is also included in the technique of multi-point distribution.

[0017] Next, that from which the decode server which decodes the distributed digital data as a downstream system, and the output unit which outputs the decoded contents with a predetermined gestalt are separated physically is assumed. That is, a decode server restores the original cryptographic key from two or more key information that distribution was received through two or more distribution paths different from digital data, and considers what performs processing of which cipher processing performed to the digital data is canceled, and processing which carries out scramble processing of the digital data with which predetermined signal processing was performed for the output to an output unit.

[0018] Thus, by having prepared the decode function of cipher processing apart from the output unit, it can do with the system configuration with which there are few updating burdens of a facility and they can be managed for a sink side. That is, also when changing a cipher system after the beginning of mission of a distribution system, as long as there is no trouble in the engine performance about the output unit which is unrelated to decode of cipher processing that what is necessary is to update only a decode server, it can be used as it is. Similarly, even when transposing an output unit to what has the more high engine performance, about a decode server without any problem, it can be used as it is. This structure is effective when reducing long-term employment cost.

[0019] But only by separating a decode function and an output unit, although it will become a very defenseless distribution model to a malfeasance, even if the digital data which flows between a decode server and output units comes to hand unjustly, the contents itself can come to hand no longer by using the data which flow between a decode server and output units as the digital data by which scramble processing was carried out.

[0020] In addition, the structure from which a malfeasance cannot arise in a decode server or an output unit is adopted. For example, except the procedure of normal, if it opens unjustly, the structure which cannot open the case of a decode server or an output server, and the structure which stops operating will be adopted. Moreover, the structure from which the cryptographic key which integrated-circuit-izes the specific processing facility performed in a decode server, and appears in process of processing, and raw digital data are made not to be taken out is adopted. It is possible

to use the electronic key which only those who have rating opened, for example as a procedure of normal here hold, and a physical key. Moreover, as an action opened unjustly, it is possible to destroy a case, for example.
[0021] (2) Explain a typical means to realize a distribution model, below a typical means to realize a distribution model. A distribution model here is premised on the distribution system which consists of an upstream system and a downstream system as mentioned above. Moreover, below, the distribution approach seen from the whole distribution model is explained. In addition, although it is expected that an upstream system and a downstream system have the common case where it is built by another entrepreneur, an employment gestalt in which the entrepreneur of an upstream system takes charge of even the processing to processing in which cipher processing performed to the digital data is canceled is not eliminated.
[0022] Various gestalten can be considered in the management gestalt of an upstream system. For example, the case where the gestalt and two or more entrepreneurs to whom a single entrepreneur manages an upstream system manage an upstream system jointly can be considered. For this reason, each processing which constitutes each following means may be performed by not only when carried out by the single entrepreneur but two or more entrepreneurs.
[0023] As a single entrepreneur, while having the right of distribution of digital data, what also undertakes the distribution enterprise of digital data is assumed here, for example. In addition, that it can consider that is single substantially may also be included in a single entrepreneur. for example, the tax law of a certain firm -- although it is not the older subsidiary, also when the associated company and subsidiary which are permitted capital-related [ fixed ] share and carry out processing, it thinks. But these are considered to be also operations by two or more entrepreneurs so that it may mention later.
[0024] When an upstream system is carried out by two or more entrepreneurs, it depends on the request on business whether each processing facility can distribute to which entrepreneur. Therefore, the configuration of the concrete hardware used by each entrepreneur and the configuration of software can consider various things according to the combination of each processing.
[0025] For example, the entrepreneur who has a right of distribution about processing until it enciphers digital data, and the processing which generates two or more key information that it responded to each distribution place performs, and if a distribution entrepreneur is made to perform only distribution of the enciphered digital data, that a cryptographic key (master key) can be known can do only with the entrepreneur who has a right of distribution. For this reason, in adopting this management gestalt, it can do with the system which is easy to hold safety for the entrepreneur who has a right of distribution. As an entrepreneur who has a right of distribution here, it thinks of the entrepreneur (if it may be an entrepreneur other than a contents maker, it contains, also when it is the same entrepreneur as a contents maker.) who acquired the right of

distribution, for example from the maker of digital data.
[0026] In addition, although reference is not made about digital watermarking with each following means, before enciphering digital data from prevention of a malfeasance or a specific viewpoint of an outflow path, it is desirable to put in digital watermarking of a proper. It is thought that it is actually put into digital watermarking in almost all cases.
[0027] Moreover, it is free that a distribution entrepreneur and the manager of a transmission network perform other cipher processing separately on the occasion of distribution of the enciphered digital data. Moreover, it is desirable, when distributing key information and a phase hand checking that it is a Shinsei distribution place, and enciphering key information with the other party's public key on it in practice by a digital certificate (that in which the certificate authority which is the 3rd person engine which can trust it carried out the digital signature) etc. expects insurance.
[0028] In addition, with the following means, the key obtained [ key / a "doubling key" and / doubling ] by dividing further in the key directly obtained from a cryptographic key by division processing shall be called "partial key." But any key is the same at the point which is a part of cryptographic key. Moreover, with the following means, the key used for enciphering a cryptographic key shall be called "multiplex key." In addition, naturally encryption processing of a cryptographic key is included, not only 1 time but when carrying out in [ many times ] superposition like 2 times and 3 times.
[0029] Moreover, when distributing key information in each means, it is also possible to use the same thing for the transmission network of key information physically with the transmission network of digital data. However, it does not carry out distributing digital data and key information at this time of day in that case, but each distribution time zone is shifted, and it is desirable to distribute in the condition same with distributing by alternative pathway in practice. If this carries out coincidence distribution of digital data and its key information through the same distribution path, since it can obtain a part of digital data and key information to coincidence by one malfeasance, it is for the danger that the code given to the part and digital data will be canceled to increase.
[0030] In addition, in any [ of each means ] case, the downstream system shall know information required to restore a cryptographic key beforehand from the key information which receives distribution, or shall be notified from an upstream system. Of course, distribution and coincidence of key information are sufficient as the timing to which the information concerned is notified from an upstream system, and another timing is sufficient as it.
[0031] (2-1) the upstream system which constitutes a distribution system from the 1st means [ 1st ] of a means, and a downstream system -- respectively -- with, propose what performs lower processing. In addition, if an upstream system may be managed as mentioned above by the entrepreneur independent which has the right of distribution of digital data, it may be managed by the distribution entrepreneur who

performs distribution of an entrepreneur and digital data which has the right of distribution concerned. Moreover, a downstream system consists of a decode server which cancels cipher processing performed to the digital data as mentioned above, and an output unit which outputs digital data with a predetermined output gestalt. These are the same also in other means to mention later.

[0032] It is the lot (not only a pair but the combination of three or more pieces is included.) of a proper to each specific person who is a distribution place the processing enciphered by the cryptographic key to which an upstream system corresponds digital data under the control, and based on the above-mentioned cryptographic key. It is the same about other means. What performs processing which generates a doubling key, processing which doubles and distributes a key or its generating information using the generated thing which digital data is another distribution path and serves as another distribution path also in mutual, and processing which distributes the digital data with which cipher processing was performed is proposed.

[0033] moreover, in a downstream system (prepared for each distribution place of every.) In the bottom of control of the decode server which can be opened only in the procedure of normal The processing which restores the cryptographic key of digital data [ / based on the doubling key or its generating information on the lot which received distribution through two or more distribution paths ], The processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled, In the only output destination change of the digital data of which the processing which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, and cipher processing were canceled In the processing which decrypts the coding processing performed to the digital data concerned, and restores the former data of digital data, and the only output destination change of the restored digital data What performs processing which carries out scramble processing and outputs the former data of digital data is proposed using the scramble key generated by the above-mentioned processing.

[0034] Moreover, the thing perform the processing of which the scramble processing performed to the digital data inputted into the bottom of control of the output unit which can be opened only in the procedure of normal from the above-mentioned decode server cancels with the scramble discharge key given from the above-mentioned decode server, and the processing output the digital data concerned at a predetermined output gestalt in the only output destination change of the digital data of which the scramble was canceled by the above-mentioned processing proposes.

[0035] In short, the 1st means the cryptographic key used for encryption of digital data Divide into each distribution place (downstream system) under the division regulation of a proper, and the doubling key of a lot (for example, three pieces) is generated. The method which distributes them using what is a distribution path

different from digital data, and serves as another distribution path also in both doubling keys, The playback system which outputs to an output unit what performed scramble processing to the digital data of which cipher processing was canceled using the cryptographic key restored from the key information which received distribution is combined.
[0036] Although this 1st means explains from a viewpoint of signal processing, it is also possible to realize by the hardware configuration equipped with these processing facilities, and it is also possible to realize the same function as software processing. It is the same about other means to mention later. In this case, hardware and software (program product of the record medium which recorded the program which performs applicable processing on the computer, the program itself, and others) are prepared about each of an upstream system and a downstream system. In addition, to hardware, a component part (circuit apparatus in a claim) called others, interface boards, semiconductor integrated circuits, etc., such as a decode server and an output unit, can be considered. [ finished product ]
[0037] By using this 1st means, unless the theft also of all the key information that remains even if the theft of either is carried out among two or more key information distributed through two or more distribution paths is carried out, the distribution model which can prevent the outflow of a cryptographic key can be offered. Since especially key information required for restoration of a cryptographic key even when the digital data with which the malfeasance person who stole a part of key information was enciphered when key information was distributed in a path (the case where it distributes in another time zone in time is included using the medium same as mentioned above.) different from digital data also comes to hand is distributed apart from digital data, the situation where raw digital data is decrypted is made more as for it to difficulty.
[0038] Moreover, with this 1st means, by having adopted the method which outputs to an output unit what carried out scramble processing of the digital data by which decode processing was carried out locally, even when using a decode server and an output unit as another equipment physically, the distribution model which can avoid certainly a possibility that raw digital data may flow out between the equipment concerned can be offered. And as the result, the development burden of a decode server or an output unit is mitigable. In this way, the fall of the price of a decode server or an output unit can be realized, and it can do with the system which is easy to introduce also for the user of distribution service. Moreover, also when long-term employment is taken into consideration, the replacement to a latest technology tends to progress at low costs, and desirable structure can be realized to an offer [ of service ], and user side. This effectiveness is the same about other means.
[0039] In addition, although premised on the cryptographic key corresponding to encryption of digital data already existing with the 1st means, you may generate within an upstream system and the cryptographic key concerned may be given from

the exterior of an upstream system. The thing of a proper is sufficient as a cryptographic key here at each digital data, and it may be common to two or more digital data. When using the former key, even if a cryptographic key is finally decoded, the damage can be limited to the digital data concerned. But even when using the latter key, the range where the damage at the time of a theft reaches can be limited by changing a key comparatively frequently. In addition, the explanation about the cryptographic key used for encryption of this digital data is the same about other means.

[0040] Incidentally as the distribution approach of the key information in the 1st means, the following can be taken, for example. For example, the approach of distributing some doubling keys of a lot through a transmission network (network), and distributing others through a record medium can be taken. Thus, if a part of key information is distributed with the gestalt of the record medium which is a truth object, it is easy to discover the theft of key information, and the countermeasures over a malfeasance can be implemented promptly.

[0041] Moreover, the approach of distributing some doubling keys of a lot through the 1st transmission network (network), and distributing others through the 2nd transmission network (network), for example can be taken. Thus, if all key information is distributed through a transmission network, time constraint which distribution of key information takes can be lessened. Moreover, key information can be distributed economically. in addition, the distribution of key information using the above transmission network (network) -- facing -- a digital certificate -- using it -- him -- the technique of distributing the key information enciphered with the public key which is checked (check of a distribution place) and the attested distribution place exhibits is desirable.

[0042] Moreover, the approach of distributing some doubling keys of a lot through the 1st record medium, and distributing others through the 2nd record medium, for example can be taken. Thus, if all key information is distributed with the gestalt of the record medium which is a truth object, the theft of key information can be made much more easy to discover, and the countermeasures over a malfeasance can be implemented promptly. Of course, a physically different medium is used for two record media. needless to say, even when it is the same about the class and reading method of a record medium, it does not matter even if it differs.

[0043] Here, to the record medium used for distribution of a doubling key, the medium (for example, a magnetic tape, a floppy (trademark) disk, a magnetic card) of a magnetic reading method, the medium (for example, CD-ROM, MO, CD-R, DVD) of an optical reading system, and semiconductor memory (a memory card (configurations, such as a rectangle mold and a square mold, are not asked.), IC card) and others can be considered. A mail system and a home delivery system are used for distribution of the record medium concerned. It thinks [ that a registered mail is chosen from a viewpoint of secrecy nature in many cases, and ] under the system of present. The

publication about the record medium for this distribution is common also about each following means. Moreover, the same is said of the record medium in the case of using for distribution of digital data.
[0044] Moreover, as the above-mentioned output unit, the recording device to an indicating equipment (for example, electronic equipment of a monitoring device, a television receiver, projector equipment, and a pocket mold), an airline printer, a loudspeaker, and a record medium etc. can be considered. Here, in the predetermined output gestalt in an output unit, if digital data is a video data, the display to the display screen and the projection to plane of projection can be considered. Moreover, if digital data is for example, audio data, the output which leads a loudspeaker can be considered. Of course, if it is audio data and complex data of a video data, two outputs will be performed to the coincidence.
[0045] (2-2) the upstream system which constitutes a distribution system from the 2nd means [ 2nd ] of a means, and a downstream system -- respectively -- with, propose what performs lower processing.
[0046] The processing enciphered by the cryptographic key to which an upstream system corresponds digital data under the control, The processing which generates the doubling key of the lot of a proper based on a cryptographic key at each specific person who is a distribution place, The generated processing which doubles and generates further two or more partial keys about a part of key or its generating information, The processing which distributes the remaining doubling keys which were not used for generation of two or more partial keys concerned, or the generating information and these partial key of those, or the generating information of those using what digital data is another distribution path and serves as another distribution path also in mutual, What performs processing which distributes the digital data with which cipher processing was performed is proposed.
[0047] moreover, in a downstream system (prepared for each distribution place of every.) In the bottom of control of the decode server which can be opened only in the procedure of normal Two or more partial keys which received distribution through two or more distribution paths, or the generating information of those, The processing which restores the doubling key which makes these and a group, or the cryptographic key of digital data [ / based on the generating information ], The processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled, In the only output destination change of the digital data of which the processing which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, and cipher processing were canceled In the processing which decrypts the coding processing performed to the digital data concerned, and restores the former data of digital data, and the only output destination change of the restored digital data What performs processing which carries out scramble processing and outputs the former data of digital data is proposed using the scramble key generated by the above-

mentioned processing.
[0048] Moreover, the thing perform the processing of which the scramble processing performed to the digital data inputted into the bottom of control of the output unit which can be opened only in the procedure of normal from the above-mentioned decode server cancels with the scramble discharge key given from the above-mentioned decode server, and the processing output the digital data concerned at a predetermined output gestalt in the only output destination change of the digital data of which the scramble was canceled by the above-mentioned processing proposes.
[0049] In short, the 2nd means the cryptographic key used for encryption of digital data Divide into each distribution place (downstream system) under the division regulation of a proper, and it considers as the doubling key of a lot (for example, three pieces). That part (for example, two pieces) is distributed as it is (one piece in this case). For example, the method which divides, generates two or more partial keys, and distributes this, The playback system which outputs to an output unit what performed scramble processing to the digital data of which cipher processing was canceled using the cryptographic key restored from the key information which received distribution is combined. Of course, it is a distribution path different from digital data, and what serves as another distribution path also in between [ each ] key information is used for distribution of these key information.
[0050] If this 2nd means is used, unless the theft also of all the key information that remains even if the theft of either is carried out among two or more key information distributed through two or more distribution paths is carried out, the distribution model which can prevent the outflow of a cryptographic key can be offered. And in the case of this 2nd means, since the distribution path of key information can be further increased rather than the 1st means, the high distribution model of safety to a malfeasance can be offered more.
[0051] In addition, a regulation common to all distribution places is sufficient as the division regulation used for generating the partial key of a lot from a doubling key, and the regulation of a proper is sufficient as it for every set of the distribution place which the regulation of a proper is sufficient as and was classified into each distribution place on condition that a specific area and others. Also in other means, it is the same.
[0052] In addition, there is also the approach of carrying out the multiplex key of some of doubling keys besides [ which divides some doubling keys further ] an approach in the generation method of a partial key here. In the case of the latter, the cryptographic key used for the enciphered key information and its encryption serves as a candidate for distribution. It is the same about other means to adopt the same structure.
[0053] Incidentally as the distribution approach of the key information in the 2nd means, the following can be taken, for example. For example, the approach of distributing some doubling keys through a transmission network (network), distributing

some partial keys generated from other doubling keys with a transmission network (network), and distributing the partial key which remains with a record medium can be taken. Thus, by distributing a part of key information with the gestalt of the record medium which is a truth object, the theft of key information can be made easy to discover and the countermeasures over a malfeasance can be implemented promptly. In addition, needless to say, which key information is sufficient as the distribution by the record medium, and it can also distribute two kinds of key information on arbitration with a respectively different record medium.

[0054] Moreover, the approach of distributing some doubling keys of a lot and all the partial keys generated from the doubling key which remains with a transmission network (network), for example can be taken. Thus, if all key information is distributed through a transmission network (network), time constraint which distribution of key information takes can be lessened. Moreover, key information can be distributed economically. in addition, the distribution of key information using the above transmission network (network) -- facing -- a digital certificate -- using it -- him -- the technique of distributing the key information enciphered with the public key which is checked (check of a distribution place) and the attested distribution place exhibits is desirable.

[0055] Moreover, the approach of distributing some doubling keys of a lot and all the partial keys generated from the doubling key which remains with a record medium, for example can be taken. Thus, if all key information is distributed through the record medium which is a truth object, the theft of key information can be made much more easy to discover, and the countermeasures over a malfeasance can be implemented promptly. Of course, the gestalten of a medium may differ and, as for the record medium used for distribution of key information, reading methods may differ, respectively.

[0056] (2-3) the upstream system which constitutes a distribution system from the 3rd means [ 3rd ] of a means, and a downstream system -- respectively -- with, propose what performs lower processing.

[0057] The processing enciphered by the cryptographic key to which an upstream system corresponds digital data under the control, It is a proper at each specific person who is a distribution place. Or the processing which generates the 2nd cryptographic key of a proper in digital data, The processing the above 1st was generated by whose 2nd cryptographic key of the above and which doubles and enciphers a key or its generating information, The processing which distributes the 1st enciphered cryptographic key concerned, its generating information and 2nd cryptographic key of the above, or its generating information using what digital data is another distribution path and serves as another distribution path also in mutual, What performs processing which distributes the digital data with which cipher processing was performed is proposed.

[0058] moreover, in a downstream system (prepared for each distribution place of

every.) In the bottom of control of the decode server which can be opened only in the procedure of normal The processing which cancels cipher processing performed to the 1st cryptographic key which received distribution, or its generating information based on the 2nd cryptographic key which received distribution through two or more distribution paths, or its generating information, and restores the 1st cryptographic key, The processing of which cipher processing performed to the digital data which corresponds using the 1st restored cryptographic key is canceled, In the only output destination change of the digital data of which the processing which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, and cipher processing were canceled In the processing which decrypts the coding processing performed to the digital data concerned, and restores the former data of digital data, and the only output destination change of the restored digital data What performs processing which carries out scramble processing and outputs the former data of digital data is proposed using the scramble key generated by the above-mentioned processing.

[0059] Moreover, the thing perform the processing of which the scramble processing performed to the digital data inputted into the bottom of control of the output unit which can be opened only in the procedure of normal from the above-mentioned decode server cancels with the scramble discharge key given from the above-mentioned decode server, and the processing output the digital data concerned at a predetermined output gestalt in the only output destination change of the digital data of which the scramble was canceled by the above-mentioned processing proposes.

[0060] The cryptographic key with which the 3rd means, in short, comes to encipher the cryptographic key (the 1st cryptographic key) used for encryption of digital data by the 2nd cryptographic key, The method which distributes the 2nd cryptographic key used for the encryption using what serves as another distribution path also in each cryptographic keys of both, using a distribution path different from digital data, The playback system which outputs to an output unit what performed scramble processing to the digital data of which cipher processing was canceled using the cryptographic key restored from the key information which received distribution is combined.

[0061] By using this 3rd means, unless the theft also of all the key information that remains even if the theft of either is carried out among two or more key information distributed through two or more distribution paths is carried out, the distribution model which can prevent the outflow of a cryptographic key can be offered. Since especially key information required for restoration of a cryptographic key even when the digital data with which the malfeasance person who stole a part of key information was enciphered when key information was distributed in a path (the case where it distributes in another time zone in time is included using the medium same as mentioned above.) different from digital data also comes to hand is distributed apart from digital data, the situation where raw digital data is decrypted is made more as for

it to difficulty.
[0062] In addition, in using the thing of a proper for each distribution person who is a distribution place as the 2nd cryptographic key, unless it carries out the theft of all the key information (the 1st cryptographic key enciphered as the 2nd cryptographic key) from a specific distribution person, the code given to the digital data cannot be canceled. That is, even if it carries out the theft of the 2nd cryptographic key of the proper addressed and distributed to a certain distribution person, and the 1st enciphered cryptographic key which was addressed and distributed to a certain distribution person, the 1st cryptographic key cannot be taken out. Of course, if the theft of the enciphered digital data is not carried out, the theft of the digital data itself is not made. In addition, it is difficult to carry out the theft of all the data, before a malfeasance is revealed as a matter of fact, and can do with a system strong against a malfeasance.
[0063] Moreover, even when the theft of the 1st cryptographic key enciphered by the 2nd cryptographic key and 2nd cryptographic key concerned when the thing of a proper was used for digital data as the 2nd cryptographic key is carried out, the damage can be limited to specific digital data (of course, it will be the requisite that the theft also of the enciphered digital data is carried out.). Needless to say, it is difficult to carry out the theft of all the data before disclosure of a malfeasance also in this case as a matter of fact, and can do with a system strong against a malfeasance.
[0064] In addition, although it is needless to say, it is peculiar about each distribution person who is a distribution place as the 2nd cryptographic key, and if the thing of a proper is used also about digital data, it can do with a system with a more difficult theft. It depends on the employment policy [ whether which an above-mentioned cryptographic key is adopted ] of the economic merit of digital data, or digital data which is a candidate for distribution.
[0065] Incidentally you may combine with the processing enciphered by the cryptographic key of other classes that what is necessary is just to perform encryption of the 1st cryptographic key once [ at least ] by the 2nd cryptographic key. Therefore, before enciphering by the 2nd cryptographic key, the 1st cryptographic key may already be enciphered. Even in such a case, there is no difference on a technique in the 1st cryptographic key being enciphered by the 2nd cryptographic key.
[0066] In addition, as the distribution approach of the key information in the 3rd means, the following can be taken, for example. For example, the approach of distributing the 1st enciphered cryptographic key through a transmission network (network), and distributing the 2nd cryptographic key through a record medium can be taken. Thus, if a part of key information is distributed with the gestalt of a record medium, it is easy to discover the theft of key information, and the countermeasures over a malfeasance can be implemented promptly. In addition, the approach of distributing the 1st enciphered cryptographic key through a record medium contrary

to an above-mentioned case, and distributing the 2nd cryptographic key through a transmission network (network) can also be taken.
[0067] Moreover, the approach of distributing the 1st enciphered cryptographic key through the 1st transmission network (network), for example, and distributing the 2nd cryptographic key through the 2nd transmission network (network) can be taken. Thus, if all key information is distributed through a transmission network, time constraint which distribution of key information takes can be lessened. Moreover, key information can be distributed economically. in addition, the distribution of key information using the above transmission network (network) -- facing -- a digital certificate -- using it -- him -- the technique of distributing the key information enciphered with the public key which is checked (check of a distribution place) and the attested distribution place exhibits is desirable.
[0068] Moreover, the approach of distributing the 1st enciphered cryptographic key through the 1st record medium, for example, and distributing the 2nd cryptographic key through the 2nd record medium can be taken. Thus, if all key information is distributed with the gestalt of the record medium which is a truth object, the theft of key information can be made much more easy to discover, and the countermeasures over a malfeasance can be implemented promptly. Of course, a physically different medium is used for two record media. needless to say, even when it is the same about the class and reading method of a record medium, it does not matter even if it differs.
[0069] (2-4) the upstream system which constitutes a distribution system from the 4th means [ 4th ] of a means, and a downstream system -- respectively -- with, propose what performs lower processing.
[0070] The processing whose upstream system enciphers digital data by the 1st cryptographic key under the control, It is a proper at each specific person who is a distribution place. Or the processing which generates the 2nd cryptographic key of a proper in digital data, Digital data is another distribution path about the doubling key or its generating information on the lot generated from the processing which generates the doubling key of a lot based on the 2nd cryptographic key of the above, the 1st cryptographic key enciphered by the 2nd cryptographic key, or its generating information and 2nd cryptographic key of the above. What performs processing distributed using what serves as another distribution path also in mutual, and processing which distributes the digital data with which cipher processing was performed is proposed.
[0071] moreover, in a downstream system (prepared for each distribution place of every.) In the bottom of control of the decode server which can be opened only in the procedure of normal The 2nd cryptographic key is restored based on the doubling key or its generating information on the lot which received distribution through two or more distribution paths. The processing which cancels cipher processing performed to the 1st cryptographic key which received distribution, or its generating information, and restores the 1st cryptographic key, The processing of which cipher processing

performed to the digital data which corresponds using the 1st restored cryptographic key is canceled, In the only output destination change of the digital data of which the processing which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, and cipher processing were canceled In the processing which decrypts the coding processing performed to the digital data concerned, and restores the former data of digital data, and the only output destination change of the restored digital data What performs processing which carries out scramble processing and outputs the former data of digital data is proposed using the scramble key generated in the above-mentioned processing.

[0072] Moreover, the thing perform the processing of which the scramble processing performed to the digital data inputted into the bottom of control of the output unit which can be opened only in the procedure of normal from the above-mentioned decode server cancels with the scramble discharge key given from the above-mentioned decode server, and the processing output the digital data concerned at a predetermined output gestalt in the only output destination change of the digital data of which the scramble was canceled by the above-mentioned processing proposes.

[0073] In short, the 4th means divides the 2nd cryptographic key, for example, uses it as the doubling key of a lot (for example, three pieces), and combines the playback system which outputs to an output unit what performed scramble processing to the digital data of which cipher processing was canceled using the method distributed with the 1st cryptographic key which had them enciphered, and the cryptographic key restored from the key information which received distribution. Of course, it is a distribution path different from digital data, and what serves as another distribution path also in between [ each ] key information is used for the distribution path of these key information.

[0074] If this 4th means is used, unless the theft also of all the key information that remains even if the theft of either is carried out among two or more key information distributed through two or more distribution paths is carried out, the distribution model which can prevent the outflow of a cryptographic key can be offered. And in the case of this 4th means, since the distribution path of key information can be further increased rather than the 3rd means, the high distribution model of safety to a malfeasance can be offered more.

[0075] In addition, the cryptographic key used for the key information which enciphers the 2nd cryptographic key besides [ which divides the 2nd cryptographic key ] an approach by still more nearly another cryptographic key, and is acquired from the 2nd cryptographic key under a predetermined division regulation as mentioned above as an approach of using for generating the doubling key of a lot, and its encryption is also included. Incidentally, a regulation common to all distribution places is sufficient as a division regulation, and the regulation of a proper is sufficient as it for every set of the distribution place which the regulation of a proper is sufficient as and was

classified into each distribution place on condition that a specific area and others. Moreover, you may be the regulation of a proper at digital data. Of course, the system by which key information cannot flow out easily much more can be built by combining the regulation about these distribution place, and the regulation about digital data.
[0076] In addition, the 2nd cryptographic key used with this 4th means also uses the same thing as the 3rd means. For example, the thing of a proper is used for each distribution person who is a distribution place as the 2nd cryptographic key. In this case, unless the theft of all the key information (the doubling key of the lot generated from the 2nd cryptographic key and the 1st cryptographic key enciphered by the 2nd cryptographic key) is carried out from a specific distribution person, the code given to the digital data cannot be canceled. That is, the 2nd cryptographic key of the proper addressed and distributed to a certain distribution person rather than the 3rd means can reduce much more the danger that a theft will be carried out.
[0077] Moreover, even when using the thing of a proper for digital data as the 2nd cryptographic key, and the theft of all the key information is carried out, in addition to the ability to limit the damage to specific digital data (it to be the requisite that the theft also of the enciphered digital data is carried out, of course.), it can fall much more in possibility itself that the theft of the 2nd cryptographic key will be carried out.
[0078] In addition, although it is needless to say, it is peculiar about each distribution person who is a distribution place as the 2nd cryptographic key, and if the thing of a proper is used also about digital data, it can do with a system with a more difficult theft. It depends on the employment policy [ whether which an above-mentioned cryptographic key is adopted ] of the economic merit of digital data, or digital data which is a candidate for distribution.
[0079] Incidentally you may combine with the processing enciphered by the cryptographic key of other classes that what is necessary is just to perform encryption of the 1st cryptographic key once [ at least ] by the 2nd cryptographic key. Therefore, before enciphering by the 2nd cryptographic key, the 1st cryptographic key may already be enciphered. Even in such a case, there is no difference on a technique in the 1st cryptographic key being enciphered by the 2nd cryptographic key.
[0080] In addition, as the distribution approach of the key information in the 4th means, the following can be taken, for example. For example, the approach of distributing the 1st enciphered cryptographic key with a record medium, distributing some doubling keys of the lot generated from the 2nd cryptographic key with a transmission network (network), and distributing the partial key which remains with a record medium can be taken. Thus, by distributing a part of key information with the gestalt of a record medium, the theft of key information can be made easy to discover and the countermeasures over a malfeasance can be implemented promptly. In addition, needless to say, which key information is sufficient as the distribution by the record medium, one kind of key information on arbitration can be distributed with a record medium, and the key information on other can also be distributed through a

transmission network (network).
[0081] Moreover, the approach of distributing the 1st enciphered cryptographic key and all the doubling keys of the lot generated from the 2nd cryptographic key through a transmission network (network), for example can be taken. Thus, if all key information is distributed through a transmission network (network), time constraint which distribution of key information takes can be lessened. Moreover, key information can be distributed economically. in addition, the distribution of key information using the above transmission network (network) -- facing -- a digital certificate -- using it -- him -- the technique of distributing the key information enciphered with the public key which is checked (check of a distribution place) and the attested distribution place exhibits is desirable.
[0082] Moreover, the approach of distributing the 1st enciphered cryptographic key and all the doubling keys of the lot generated from the 2nd cryptographic key through a record medium, for example can be taken. Thus, if all key information is distributed through a record medium, the theft of key information can be made much more easy to discover, and the countermeasures over a malfeasance can be implemented promptly. Of course, the gestalten of a medium may differ and, as for the record medium used for distribution of key information, reading methods may differ, respectively.
[0083]
[Embodiment of the Invention] (1) The fundamental example of a configuration of the business model which this application specification assumes to business model (1-1) general example drawing 1 is shown. This business model consists of a distribution person who is the informer of digital data, and a specific person who is the sink of digital data. In addition, drawing 1 expresses the case where it consists of two persons of the distribution entrepreneur 2 to whom a distribution person undertakes the distribution enterprise of the right person 1 of distribution, and digital data which has the right of distribution of digital data. Although it is thought that there is not little this also when the right person of distribution and a distribution entrepreneur are the same people, also when a distribution person is constituted by two or more persons more than it, it is because it is thought that it is not few.
[0084] Moreover, the right person 1 of distribution also has the case of the consortium of the right person of distribution, and a contents maker, when it is the contents maker itself [ besides in the case of being those who yielded and received contents, i.e., the right of distribution of digital data from the contents maker ]. On the other hand, an individual and an entrepreneur (for example, theater entrepreneur) correspond to a specific person.
[0085] As mentioned above, the case where an upstream system (seeing from data flow semantics of the system of the upstream) consists of a system of the right person of distribution and a distribution entrepreneur's system here, and a downstream system (seeing from data flow semantics of the system of the

downstream) consists of a specific person's systems is explained.
[0086] The digital data assumed for distribution has alphabetic data (for example, a text, a notation, a graphic form), audio data (for example, voice, a musical piece), a video data (for example, a still picture, an animation), audio data, the complex data (for example, a movie, a program) of a video data, program data, database data, and other digital data. Of course, such attached information (for example, there is information about ID (identification information on a medium) called metadata, photography time, a location, a person, a condition, etc.) may also be included.
[0087] Generally, for distribution of digital data, the network 3 for high-speed distribution suitable for a transmission band distributing large mass data is assumed ( drawing 1 ). In this drawing 1 , the system which distributes digital data for the digital data as contents to the specific persons A and B etc. through delivery and the network 3 for high-speed distribution is shown to the electronic distribution entrepreneur 2 from the contents work firm 1. However, distribution with the gestalt by the record medium of CD-ROM, or DVD and others is not eliminated. A broadcasting satellite and the broadband-transmission network of an optical fiber and others are used for the network 3 for high-speed distribution. It gets down at least and these use about a direction the thing in which mass transmission is possible. But the bidirectional transmission network in which transmission in the uphill direction is also possible may be used.
[0088] The data 8 of DS as shown in drawing 2 are distributed to the network 3 for high-speed distribution. Here, although picture 8A of a key is expressed to the data 8 of drawing 2 , this expresses the case where a cryptographic key is hung uniquely, in order that a network provider (he is not a distribution entrepreneur) may secure the secrecy nature of the communication service which self offers. Therefore, this key may not be hung.
[0089] But the right person of distribution who gives top priority to the safety to the malfeasance of digital data, and the distribution entrepreneur will choose as data uniquely the network operator who performs cipher processing also on the network, and are considered to choose the network operator who performs cipher processing with high nearby safety in it. In addition, although omitted in drawing 2 , when distributing data 8 in fact, a required header exists.
[0090] The part of the contents surrounded with the broken line of drawing 2 is equivalent to the data distributed by the above-mentioned electronic distribution entrepreneur 2. In the case of drawing 2 , file allocation table (FAT:File Allocation Table) 8B which shows data or the storing information on a file, operating data 8C including the service condition (the refreshable period for every distribution place and distribution place and conditions of the count of playback and others) of digital data, image data 8D, and voice data 8E are stored in the data concerned.
[0091] the picture of the key each data is locked here means that each [ these ] data is protected by cipher processing which the right person of distribution and the

distribution entrepreneur performed by or the both co-operation one of ones of these. Here, generally as for the cryptographic key given to each data, the same cryptographic key is used. However, it is also possible to hang a cryptographic key which may adopt a different cryptographic key for every (every [ for example, ] image data) classification of data, and is different irrespective of the classification of data for every (every [ for example, ] image data and voice data which differs in a codec) data.

[0092] As shown in drawing 2 , in this distribution model, the method which distributes a certain contents in a multi-format is adopted. That is, the approach of preparing and distributing two or more kinds of image data and voice data which differ in a coding decryption method (codec) about one contents which are the candidates for distribution is adopted. In the case of drawing 2 , signs that three kinds of image data which differ in a codec method about a certain image contents are distributed are expressed. As a codec method here, MPEG (Moving Picture Experts Group), and wavelet (Wavelet) and others can be considered, for example.

[0093] Thus, image contents are encoded and distributed by two or more kinds of codec methods for giving a degree of freedom to the system configuration by the side of the specific person who receives distribution. Thereby, a specific person does not need to adopt the codec system of dedication only for use of digital distribution service, and can use the system to which self is used as it is. Thus, since the selection range of digital data will not be restricted if there is an advantage which is not restricted to what holds the system of specification [ a specific person (distribution place of data) ] when it sees from a distribution person side, and it sees from a specific person side, the distribution method by multi-format has the advantage which can use the existing facility effectively.

[0094] The same is said of voice data 8E. In the case of drawing 2 , the data encoded by two kinds of codec methods are stored. There are for example, MPEG and others in a codec method here.

[0095] In addition, in the case of the business model of drawing 1 , the data which can receive the home expressed as the specific person A are the image codec VCD1. The image data and the voice codec ACD1 which were encoded Since it is the encoded voice data, they are alternatively extracted based on the information on FAT out of the data 8 which received distribution, or are reproduced. The data which the entrepreneur who expressed the specific person B needs on the other hand are the image codec VCD2. The image data and the voice codec ACD2 which were encoded Since it is the encoded voice data, they are alternatively extracted based on the information on FAT out of the data 8 which received distribution, or are reproduced. But it must not always distribute in a multi-format and the information on the combination of the format made required for every distribution place may be distributed.

[0096] It is explanation about the digital data with which the above receives

distribution through the network 3 for high-speed distribution. next, conditional [ which is given to the digital data concerned ] -- the distribution path of a cryptographic key required to cancel access processing (Conditional Access), i.e., cipher processing performed to the digital data, is explained. In drawing 1 , two, a wide area network (transmission medium) 4 and a record medium 5, are used as a distribution path of a cryptographic key. That is, drawing 1 expresses an example of the distribution method which adopts the method which distributes the part electronically through a wide area network 4 when you need at least two kinds of key information for restoring a common key, and distributes the part which remains physically through a record medium 5.

[0097] In addition, the wide area network 4 here assumes the transmission network in which two-way communication is possible. For example, a public network (for example, the Internet network, an ATM network, a packet communication network) and a dedicated line network can be considered. Moreover, a record medium 5 assumes the medium of a magnetic reading method, the medium of an optical reading system, and semiconductor memory and others, as above-mentioned The means for solving a technical problem described. It is also as above-mentioned to use a mail system and a home delivery system for the distribution.

[0098] In addition, in the following explanation, it is assumed that the cryptographic key given to digital data is common about all distribution places, and the key information on the lot distributed to each distribution place according to an individual is peculiar to each specific person. This is because the cryptographic key hung on the digital data cannot be restored, unless all the key information addressed and distributed to a certain specific person by adopting the key information on a proper for every specific person comes to hand. By adopting such structure, it is made as for this business model to a more difficult thing or all key information coming to hand unjustly with what requires time amount that all key information comes to hand unjustly.

[0099] Incidentally in the above-mentioned case, the cryptographic key used for encryption of each digital data was made common to all distribution persons, but the cryptographic key used for encryption of each digital data can also be made into the thing of a proper for every distribution place. Moreover, in the above-mentioned case, the key information on the lot distributed to each distribution place according to an individual is considering as the thing of a proper at each distribution place, but it can also consider as the thing of a proper at each digital data.

[0100] Incidentally, as for the cryptographic key hung on digital data, it is desirable that it is peculiar to the contents which are the candidates for distribution. Even if all key information flows out unjustly as mentioned above and this succeeds in decode of digital data, it is because damage can be limited to specific contents. Of course, it is not indispensable that the cryptographic key concerned is peculiar for every contents, and using a common cryptographic key is also considered about two or more contents.

In short, the secrecy nature to a malfeasance should just increase as the whole system, and each cryptographic key is not limited to a specific regulation. Moreover, the height of secrecy nature changes also with contents which are the candidates for distribution, and changes also with policies by the side of a distribution person.
[0101] Next, a distribution path is explained. Fundamentally, for distribution of key information, as shown in drawing 1 , what differs in a medium is assumed like a network and a record medium. This is based on the special feature of the following which each distribution path has.
[0102] First, in the case of a network, it has the advantage that distribution of key information can be performed immediately. However, when the theft of the key information is carried out, there is a fault that discovery is difficult. On the other hand, although it has the fault that it takes predetermined time amount for a specific person to receive distribution of key information in the case of a record medium, since the theft of key information can be checked physically, there is an advantage of being easy to discover a theft.
[0103] So, in many business models assumed on this application specifications, the combination of distribution through a network and the physical distribution by the record medium is assumed. But it is based on a general reason, and the above should just distribute all key information through a network, when the distribution using a network does not have fear of a malfeasance, either, or when difficult. Moreover, when there are period-allowances by distribution of digital data from distribution of key information, all the key information can also be distributed using a record medium.
[0104] There is no constraint technical about the code technique used for cipher processing of digital data incidentally, and it is applicable also about various kinds of techniques in which it will appear in the future, not to mention various kinds of techniques known at the time of application. Since a cipher system is not asked, it can do with the business model which cannot be easily influenced of a technical life. Moreover, since the technique of the employment that time highest can always be chosen, it can do with a business model strong against the part and a malfeasance.
[0105] Moreover, generally the key information distributed through two paths of a wide area network 4 and a record medium 5 in drawing 1 assumes the group of the doubling key (partial key) of a lot divided by the division pattern of a proper for every distribution place, or the group of the cryptographic key enciphered with the multiplex key of the proper generated for every distribution place, and a multiplex key, as explained in The means for solving a technical problem.
[0106] (1-2) The concrete example of a business model is shown in example drawing 3 . This is a thing about the business model which distributes movie contents electronically. There is nothing that that to which the both sides by the side of the theater which receives distribution with the entrepreneur who has the right of distribution of movie contents are fully satisfied does not have, and resulted in practical use, although, as for this kind of business model, various kinds of business

model proposals are offered towards that implementation from the former. Then, it considers applying the distribution model of this application specification.
[0107] In the case of the business model shown in drawing 3 , the contents work firm 1 of drawing 1 changes to motion picture production company 1a, and changes the specific persons 6 and 7 who receive distribution of digital data to Theaters A and B. In addition, in the case of drawing 3 , the process (telecine process: Film to Video Conversion) 9 which changes into an electronic image the film image offered from motion picture production company 1a as a configuration peculiar to movie contents is expressed. Moreover, although not distinguished by a diagram, the movie theater where Theaters A and B are called a large-scale movie theater, a small-scale movie theater, and the so-called cinema complex is assumed.
[0108] (2) The example of a functional-block configuration of the distribution system which realizes the example of distribution system above-mentioned business model is shown. In addition, each example of a system corresponds to either the 1st explained by The means for solving a technical problem - the 4th means. Of course, although there is also a publication partially limited to the specific function since it is an example of an operation gestalt, it is not restricted to these as above-mentioned.
[0109] (2-1) The 1st example of a distribution system for realizing an above-mentioned business model to the 1st example drawing 4 of a distribution system is shown. In addition, the 1st example of a distribution system corresponds to the 1st above-mentioned means. The system concerned consists of an upstream system and a downstream system. Let an upstream system here be the complex system of the system the entrepreneur's [ who has the right of distribution of contents ] 1, and the electronic distribution entrepreneur's 2 system. Of course, a single entrepreneur's system is not eliminated as mentioned above, and the complex system by three or more persons' entrepreneur is not eliminated. On the other hand, let a downstream system be the system of a proper for every specification person which receives distribution of digital data.
[0110] (2-1-1) conceptual **** -- explain the conceptual configuration of the 1st example of a distribution system concerned first. The 1st model which paid its attention to distribution of digital data, and the 2nd model which paid its attention to the sink side of digital data are contained in this 1st distribution system.
[0111] (1) The upstream system seen as the 1st model [ 1st ] of a model The processing which generates the cryptographic key of a proper in each digital data, and the processing which enciphers digital data by the corresponding cryptographic key, The processing which generates the doubling key of the lot of a proper based on the above-mentioned cryptographic key at each specific person who is a distribution place, The generated processing which doubles and distributes a part of key or its generating information to each specific person through a transmission network, Generated processing which doubles and writes the remaining part in the record medium only for keys for the distribution in the gestalt of a record medium among a

key or its generating information, and processing which distributes the digital data with which cipher processing was performed according to the distribution schedule are performed.

[0112] On the other hand, the downstream system received distribution through the transmission network, and performs processing which restores the cryptographic key of a proper to digital data [ / based on a part of key or its generating information, and the remaining part that received distribution with the gestalt of a record medium ], and processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled.

[0113] The 1st model adopts the method which, in short, divides into each distribution place (downstream system) the cryptographic key used for encryption of digital data under the division regulation of a proper, generates the doubling key of a lot, distributes the part through a transmission network, and distributes the remainder with the gestalt of a record medium.

[0114] (2) The decode server of the downstream system seen as the 2nd model [ 2nd ] of a model The processing which restores the cryptographic key of a proper to digital data [ / based on the remaining part which received distribution through the transmission network and received distribution with a part of key or its generating information, and the gestalt of a record medium ], The processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled, In the only output destination change of the digital data of which the processing which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, and cipher processing were canceled In the processing which decrypts the coding processing performed to the digital data concerned, and restores digital data, and the only output destination change of the restored digital data Processing which carries out scramble processing and outputs digital data is performed using the scramble key generated by the above-mentioned processing.

[0115] At this time, the output unit of a downstream system adopts the processing of which the scramble processing performed to the digital data inputted from a decode server is canceled with the scramble discharge key given from the decode server, and the processing which outputs the digital data concerned with a predetermined output gestalt in the only output destination change of the digital data of which scramble processing was canceled by the above-mentioned processing.

[0116] The 2nd model can be called what adopts the playback system which performs scramble processing to the digital data of which cipher processing was canceled using the cryptographic key restored in short from the key information which received distribution, and is outputted to an output unit.

[0117] In addition, whenever the scramble key and scramble discharge key which are generated by the decode server may be the same about the same digital data and cancel cipher processing, you may make it generate the key of a proper. As a cure to

a malfeasance, latter one is desirable.
[0118] Moreover, as an output unit, the recording device to an indicating equipment (for example, electronic equipment of a monitoring device, a television receiver, projector equipment, and a pocket mold), an airline printer, a loudspeaker, and a record medium etc. can be considered.
[0119] Here, in the predetermined output gestalt in an output unit, if digital data is a video data, the display to the display screen and the projection to plane of projection can be considered. Moreover, if digital data is for example, audio data, the playback which leads a loudspeaker can be considered. Of course, if it is audio data and complex data of a video data, two outputs will be performed to the coincidence.
[0120] In addition, a component part like the circuit apparatus (for example, an interface board, a semiconductor integrated circuit, etc.) which realize an applicable function besides the so-called finished product is also contained in the above decode server and output unit.
[0121] (2-1-2) In the case of system configuration drawing 4 , an upstream system consists of the contents server 11, the contents coding section 12, the encryption section 13, the sending-out server 14, the contents management server 15, the key generating section 16, a distribution place management server 17, the doubling key generation section 18, and the write-in section 19.
[0122] Although it does not dare specify whether each of these components in an upstream system are prepared in which system in an entrepreneur in drawing 4 , it is because it becomes the selection on business how this distributes each component to each entrepreneur. In addition, since the method of allocation of each component or arrangement is a matter which is common also about the example of an alien system, the term of a latter "employment gestalt assumed by each system" explains it separately.
[0123] On the other hand, a downstream system consists of the receiving server 31, a read station 32, a decode server 33, and an output unit 34 (descrambling section 34A). Among these, the decode server 33 consists of a decode function part 35 (decryption section 35A, key restoration section 35B, contents decryption section 35C, scramble section 35D), a scramble control section 36, and the output log Management Department 37 further.
[0124] In addition, it is also possible to realize each of these components as hardware of dedication, respectively, and realizing as one function of software is also possible.
[0125] Moreover, the arrow head shown by the thick wire expresses among drawing the transmission line where transmission capacity is large, and the arrow head shown with a thin line expresses the comparatively small transmission line of transmission capacity. But it is the system configuration assumed at present, and it is relative whether transmission capacity is large or small. Moreover, the distribution path of the doubling key shown by the arrow head of a thin line at present is also good also as what has large transmission capacity.

[0126] (2-1-3) **** of each function part -- explain first each function part which constitutes an upstream system. The contents server 11 is equipment which considers are recording of the digital data which received offer through the record medium ( drawing 4 magnetic tape) or the transmission line as the main functions. For this reason, it has mass storage equipment. In addition, the server concerned takes a computer configuration.
[0127] That is, the server concerned takes a configuration equipped with the processor which realizes a control function and a calculation function, the store which memorizes data required for activation of signal processing, the input unit which inputs data, and a program and a command from the exterior, and the output unit which outputs a processing result outside.
[0128] The contents coding section 12 is equipment which considers coding processing of compression coding and others of digital data as the main functions. For example, coding processing of MPEG conversion, Wavelet conversion, and others is performed. In addition, two or more coding processings in which only one kind generally is not performed but coding processing is widely adopted at the time of employment are performed. Consequently, two or more coding processed data are generated to one digital data. In addition, processing which spaces through voice or image data and embeds information is performed between the contents server 11 and the contents coding section 12. This contents coding section 12 may be constituted using the hardware of dedication, and may be realized as treatment on the software of the computer by which the program which realizes a function equivalent to the hardware concerned is installed.
[0129] The encryption section 13 is equipment which performs cipher processing to the digital data which received offer of the cryptographic key of a proper in contents from the key generating section 16, and contents coding processing ended using the cryptographic key concerned. The cipher system used here should just use what is widely adopted at the time of employment.
[0130] For example, cipher processing of DES (Data Encryption Standard), and FEAL (Fast Data Encipherment Algorithm) and others is performed. Cipher processing here is performed according to an individual about each of operating data and contents data. If reference is made by reference, cipher processing about contents data will be performed for each [ which was generated in the contents coding section 12 ] coded data of every.
[0131] In addition, the encryption section 13 may also be constituted using the hardware of dedication, and you may realize as a processing facility of software which makes a computer realize an equivalent function.
[0132] the sending-out server 14 is equipment which realizes the function which accumulates the digital data (conditional -- access processing was performed) with which encryption processing was performed so that only a specific person could view, listen or record in storage equipment, and the function outputted to the network 3 for

high-speed distribution according to a distribution schedule. An output function here is realized by the sending set equipped with a broadband-transmission function or a rate control function.
[0133] Although distribution of the data using the network 3 for high-speed distribution assumes the distribution of an are recording mold which now used Nighttime, streaming distribution etc. is assumed in the future when improvement in transmission speed is expected.
[0134] In addition, when performing distribution of digital data with the gestalt of a record medium, the output function mentioned above is realized by the recording device which stores digital data in a predetermined record medium.
[0135] The contents management server 15 is equipment which communicates with the contents server 11 and newly performs registration processing of reception beam contents, retrieval processing of contents, file division processing, and others. The server concerned also takes a computer configuration. In the server concerned, the cryptographic key information generated for every contents is managed. For example, the relation between contents and a corresponding cryptographic key is managed as a database.
[0136] The key generating section 16 is a means which is a candidate for distribution to generate the cryptographic key of a proper for every digital data. The cipher system used for generating of a cryptographic key uses what is widely adopted at the time of employment. That is, unjust decode follows the newest difficult encoding technology.
[0137] The distribution place management server 17 is equipment which manages with a database the information on the cryptographic key generated for every contents for every operating data of a distribution place, distribution conditions, and others, or distribution place. The information on an estimated usable period, and the count of output possible and others is included in distribution conditions here. Moreover, the server concerned also takes a computer configuration.
[0138] The distribution place management server 17 can consider others, when preparing only in the system of the right person 1 of contents distribution, preparing only in the electronic distribution entrepreneur's 2 system, and preparing in both system. It is because it is a selection matter on business who, as for this, distributes the key information on a proper to each distribution place. However, it cannot so be overemphasized that there are few entrepreneurs who can know key information that the secrecy nature seen from the whole system increases. Although it is thought that it is generally arranged in the system of the right person 1 of contents distribution, according to the management gestalt of business, it may be arranged in the system of the entrepreneur of an electronic distribution entrepreneur and others.
[0139] The distribution place management server 17 in the drawing of drawing 4 and others is constituted so that the output log of a downstream system may be gone up and it can receive through a circuit (the communication line of the Internet, or the

telephone line and others is generally used.). The distribution place management server 17 manages the output hysteresis (output time, the count of an output, a period, incidental information (a number, an age group, etc. of the existence of a trouble, and a contents viewer) in addition to this) of a distribution place (addressee side) based on the output log concerned. For this reason, the distribution place management server 17 is equipped with a non-illustrated database or the output hysteresis function manager section.

[0140] But these databases and the output hysteresis function manager section may be prepared apart from the distribution place management server 17. In addition, total processing (statistics processing is also included.) and analysis processing of an output log are good also as what transmits the result which could perform by the upstream system which received the notice of an output log, and the downstream system performed beforehand.

[0141] Thus, by managing the output log (activation fact) of a downstream system by the upstream system, the circulation situation of contents is made as a monitor is possible. Moreover, it can be used for grasping a commercial-scene trend (a box-office record, epidemia, an inclination, others). But an upstream system here may be an upstream system of a wide sense, and may be entrepreneurs other than the entrepreneur who has the right of distribution of digital data, or an electronic distribution entrepreneur, for example, the entrepreneur who investigates the output trend of contents.

[0142] In addition, the distribution place management server 17 does not need to perform reception of an output log, and other electronic equipment may receive. Moreover, an output log here needs to display no information (for example, output time etc.) mentioned above, and one of the arbitration or the combination of arbitration may be notified. By the way, although the case where begin drawing 4 and an output log is notified to an upstream system from a downstream system in each drawing is expressed, it is also possible to consider the distribution system which does not always need to notify and does not notify an output log.

[0143] The doubling key generation section 18 is equipment which divides the cryptographic key A generated for every contents by the division pattern of a proper for every distribution place, and generates the doubling keys A1 and A2 of a lot. For example, if there are 1000 specific persons who become a distribution place, 1000 sets of doubling keys A1 and A2 will be generated. The generated doubling key is given to the distribution place management server 17 and the predetermined message distribution processing section by the doubling key generation section 18. In the case of this system, the doubling key generation section 18 gives the doubling key A1 to distribution through a network in the non-illustrated communications department, and gives the doubling key A2 which remains to distribution through a record medium at the write-in section 19.

[0144] The write-in section 19 is equipment for having received the notice and writing

a key A2 in a predetermined record medium. The drive according to a record medium is formed in the write-in section 19. The medium of a magnetic reading method, the medium of an optical reading system, and the medium of semiconductor memory and others are used for a record medium. In addition, destination information required for distribution of a record medium is given from the distribution place management server 17. The same is said of the communications department which is not illustrated [ above-mentioned ]. However, in the case of the communications department, the address on a network is given.

[0145] Next, each function part which constitutes a downstream system is explained. the receiving server 31 is equipment realized in the reception function of digital data (conditional -- access processing was performed) to in_which encryption processing was performed so that only a specific person might view, listen or record, the function which accumulates the digital data which received distribution in storage equipment, and the function outputted to the decode server 33 according to a playback schedule. A reception function here is equipped also with the function to perform the error correction included in received data.

[0146] In addition, when receiving distribution of digital data with the gestalt of a record medium, the reception function mentioned above is realized by the reader which reads digital data in a predetermined record medium.

[0147] A read station 32 is equipment for reading in a record medium the doubling key A2 distributed with the gestalt of a record medium. The thing according to a record medium is used for a drive here. Moreover, although not expressed all over drawing, the communications department is established in reception of the doubling key A1 which receives distribution through a wide area network.

[0148] While the decode server 33 performs processing of which cipher processing performed to the digital data is canceled, and processing which decrypts the coding processing performed to the digital data of which the code was canceled, it is equipment which performs local scramble processing so that the restored raw digital data may not be outputted to the equipment exterior as it is.

[0149] The decode server 33 may be constituted using the hardware of dedication, and may be realized as a processing facility of software which makes a computer realize an equivalent function. Incidentally, if it opens unjustly, except the procedure of normal, the structure which cannot open the case, and the structure which stops operating will be used for the decode server 33 concerned, in order to protect digital data from the malfeasance by the malicious specific person. The existing technique is used about these structure.

[0150] Especially about the decode function part 35 (decryption section 35A, key restoration section 35B, contents decryption section 35C, scramble section 35D), since important information (a cryptographic key and raw digital data) flows between each functional block, it is important, and the functional-block part concerned is semiconductor-integrated-circuit-ized, or the cure for eliminating a malfeasance will

adopt the structure which cannot open the case, and the structure which stops operating except a regular procedure, if it opens unjustly.
[0151] Here, decryption section 35A is a function part which cancels cipher processing (conditional access processing) performed to the digital data read from the receiving server 31 using the cryptographic key given from key restoration section 35B. It can also realize by the hardware of dedication and the function concerned can also be realized as a function on software.
[0152] Key restoration section 35B is a function part which realizes the function which restores the cryptographic key which can cancel cipher processing which received distribution through the network, received distribution with the gestalt of a key A1 and a record medium, and is performed to the digital data based on the key A2. As for the restored cryptographic key, period maintenance of predetermined is carried out under management of key restoration section 35B. The record medium of nonvolatile memory, and a hard disk and others is used for the check concerned.
[0153] Moreover, key restoration section 35B reads operating data 8C attached to the digital data concerned, before decoding the code of the digital data read from the receiving server 31, and it also performs the judgment of whether the playback conditions (service condition) defined by the operating data 8C concerned are fulfilled at each time.
[0154] Here, when playback conditions are fulfilled, while key restoration section 35B gives a code discharge enabling signal to decryption section 35A, it gives the generating signal or output enabling signal of a scramble key to the scramble control section 36. On the other hand, key restoration section 35B gives the generating inhibiting signal or output inhibiting signal of a scramble key to the scramble control section 36 while giving a code discharge inhibiting signal to decryption section 35A, when playback conditions are not fulfilled.
[0155] The thing corresponding to the codec method with which every specific person has adopted contents decryption section 35C is used. The function concerned and realizing as hardware of dedication are also possible, and realizing as one function of software is also possible. The raw digital data before encryption processing is restored as a result of signal processing of contents decryption section 35C.
[0156] Scramble section 35D is equipment for performing scramble processing, as the digital data restored by contents decryption section 35C is not outputted with a gestalt as it is. The function concerned and realizing as hardware of dedication are also possible, and realizing as one function of software is also possible.
[0157] In addition, in the case of drawing 4 , it is also possible to form [ in / for the scramble control section 36 / the exterior of the decode function part 35 ] the scramble control section 36 as one function in the decode function part 35.
[0158] The scramble control section 36 generates the descrambling key which makes a scramble key, this, and a pair, when generating of a scramble key is permitted by key restoration section 35B. In addition, the enabling signal given to the scramble

control section 36 from key restoration section 35B may include information, such as not only the information mere authorization and that a permission is not granted but output time, and a period. Moreover, as a drawing destructive line shows, in making external connection of the scramble control section 36 to contents decryption section 35C and others, it attests each other between the function parts concerned, and a scramble key may be made to be published only when it is admited that the other party is Shinsei.

[0159] in addition, for the generating approach of a scramble key and a descrambling key How (how to output the scramble key memorized fixed and a descrambling key) for it not to be based on the difference in contents, but to always generate the same scramble key etc., How (approach held while being generated at every output of new contents and fulfilling predetermined playback conditions) to generate a different scramble key for every contents etc., There is the approach (how to generate a scramble key which is different whenever it cancels the code of contents) of generating a different scramble key at every playback output etc. Injustice becomes difficult in the sequence of the 3rd approach, the 2nd approach, and the 1st approach at the order of the publication from a viewpoint of the defense function to a malfeasance.

[0160] Incidentally, the scramble control section 36 generates a scramble key and a descrambling key suitably also during the output to the output unit 34 of digital data, when adopting a commuter's ticket or the specification changed irregularly for a scramble key while outputting one contents.

[0161] Moreover, although it is not drawn in the drawing of drawing 4 and others so that the output log Management Department 37 may be notified of generating situations, such as a scramble key, from the scramble control section 36, you may make it give the output log Management Department 36 this management information. By giving the output log Management Department 37 such information, a scramble key etc. can supervise whether it is what was generated unjustly.

[0162] The output log Management Department 37 is equipment which manages the output log in an output unit 34 in order to supervise the unjust output from an output unit 34. The function concerned and realizing as hardware of dedication are also possible, and realizing as one function of software is also possible. The output log Management Department 37 notifies an output log to the distribution place management server 17 which constitutes an upstream system through a communication line. Consequently, each specific person's playback output situation can be separately supervised also by the upstream system. Moreover, it can use also for discovery of a malfeasance.

[0163] In addition, although the output log here assumes the raw data generated or inputted by the downstream system, in the equipment of the output log Management Department 37 and others concerned, total processing (statistics processing) and the thing by which analysis processing was carried out are sufficient as it. Incidentally,

when including incidental information, such as the number of contents viewers, and an age group, as information on an output log, the information concerned shall be given from non-illustrated an input means and a processor.

[0164] Finally, the configuration of an output unit 34 is explained. The thing [ output unit / 34 ] according to digital data is used. If it is an image system, a display and projection equipment can be considered, and a loudspeaker can be considered if it is a voice system. Anyway, an output unit 34 is equipped with descrambling section 34A other than the original function part.

[0165] Descrambling section 34A is functional equipment for canceling the scramble processing performed to the digital data given from the decode server 33. The function concerned and realizing as hardware of dedication are also possible, and realizing as one function of software is also possible. The descrambling section 34A concerned consists of a semiconductor integrated circuit and a board member.

[0166] Also in this output unit 34, about the signal outputted from descrambling section 34A, since only a static protection feature like digital watermarking is given, if it opens unjustly, except the procedure of normal, the structure which cannot open the case of an output unit, and the structure which stops operating will be adopted.

[0167] (2-1-4) Explain briefly distribution actuation of the digital data in the example of a distribution system of the distribution actuation 1st of digital data. In the system concerned, if new digital data is registered into the contents server 11, the cryptographic key of a proper will be generated under management of the contents management server 15 at the contents concerned. Next, the created cryptographic key doubles, it is given to the key generation section 18, and the doubling key of a proper is generated by each distribution person with the division pattern of a proper.

[0168] Here, the division pattern of a proper may be the same as each distribution person irrespective of the difference in contents, and a different division pattern for every contents may be adopted. Anyway, in the example of a system of drawing 4 , the doubling key of a proper is generated by contents for every specific person.

[0169] Then, the generated doubling keys A1 and A2 are distributed in advance in advance of transmission of digital data. In the case of this system, the doubling key A1 is distributed for the doubling key A2 through a network with the gestalt recorded on the record medium. But it must not always be carried out in advance of distribution of digital data. A key required for discharge of cipher processing may be performed after distribution of digital data.

[0170] The downstream system which received distribution of a key together with the digital data reads digital data according to a predetermined output schedule, and cancels cipher processing by the restored cryptographic key. Then, the thing concerning the codec method which suits a specific person's system configuration among the digital data of which cipher processing was canceled is decrypted alternatively, and scramble processing about a decode result is performed by the decode server 33.

[0171] Then, from the decode server 33, the digital data with which scramble processing was performed is outputted to an output unit 34. In an output unit 34, discharge of scramble processing is performed by the descrambling key given from the scramble control section 36, and the output of contents is performed by the desired gestalt. In addition, this output situation is notified to an upstream system by the output log Management Department 37 as an output log. a notice here may be performed for every output of contents -- it may carry out (that is, it is attached to one output and notified once), and the print-out of multiple times may be notified collectively (for example, an output situation list may be outputted to day by day [ 1 ]).

[0172] (2-1-5) the effectiveness acquired by the 1st example of a distribution system -- as mentioned above, according to the 1st example of a distribution system, by having made the distribution path of a doubling key into plurality, even if the theft of one of the doubling keys is carried out, unless the theft also of another side will be carried out, the distribution model which can prevent the outflow of a cryptographic key can be offered. Since especially key information required for restoration of a cryptographic key even when the digital data with which the malfeasance person who stole some doubling keys was enciphered when a doubling key was distributed in a path (the case where it distributes in time when another is included using the transmission medium same as mentioned above.) different from digital data also comes to hand is distributed apart from digital data, it can avoid certainly the situation where raw digital data is decrypted.

[0173] Moreover, by having adopted the method which performs scramble processing as the digital data of which cipher processing was canceled, separation with the server equipment which performs a decode function, with sufficient defense capacity over a malfeasance held, and the output unit which performs a regenerative function is realizable.

[0174] It can be coped with by replacing only the decode server 33 to change the codec method dealt with when a cipher system with high safety appears by the employment back especially. Moreover, even if the codec method which a specific person deals with is what, since the data outputted to an output unit 34 from the decode server 33 are unified into the data by which scramble processing was carried out, they can share an output unit 34 by two or more codec methods.

[0175] This also means that the development costs of an output unit 34 end few. or [ namely, / that it can open only in a regular procedure while carrying descrambling section 34A in the output unit 34 of a general-purpose mold ] -- or since what is necessary is just to carry the structure which does not operate, low-pricing of an output unit 34 is realizable. Therefore, when an output unit with the high engine performance is developed by the employment back, or when what has high reappearance resolution is developed, for example, replacement of equipment tends to progress.

[0176] In this way, it can be satisfied with coincidence of the safety to a malfeasance, and economical efficiency when employing a system.
[0177] (2-2) The 2nd example of a system for realizing an above-mentioned business model to the 2nd example drawing 5 of a distribution system is shown. Drawing 5 attaches and expresses the same sign with a corresponding point with drawing 4 here. The downstream system which constitutes the system concerned is the same as the 1st example of a distribution system so that drawing 5 and drawing 4 may be understood by comparison. In addition, the 2nd example of a distribution system corresponds to the 2nd above-mentioned means.
[0178] (2-2-1) conceptual **** -- explain the conceptual configuration of the 2nd example of a distribution system concerned first. The 1st model with which its attention was paid to distribution of digital data also in this 2nd distribution system, and the 2nd model which paid its attention to the sink side of digital data are contained.
[0179] (1) The upstream system seen as the 1st model [ 1st ] of a model The processing which generates the cryptographic key of a proper in each digital data, and the processing which enciphers digital data by the corresponding cryptographic key, The processing which generates the doubling key of the lot of a proper based on a cryptographic key at each specific person who is a distribution place, The generated processing which doubles and generates further two or more partial keys about a part of key or its generating information, The processing which distributes the part or its generating information on the generated partial key to each specific person through the 1st transmission network, Processing written in the record medium only for [ the remaining part or its generating information on the generated partial key / object / for the distribution in the gestalt of a record medium ] keys, Processing which distributes the remaining doubling keys which were not used for generation of a partial key or the generating information of those to a specific person through the 2nd transmission network, and processing which distributes the digital data with which cipher processing was performed according to the distribution schedule are performed.
[0180] The partial key with which the downstream system received distribution through the 1st transmission network on the other hand, or its generating information, The partial key which received distribution with the gestalt of a record medium or its generating information, and the processing which received distribution through the 2nd transmission network and restores the cryptographic key of a proper to a key or digital data [ / based on the generating information ], Processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled is performed.
[0181] A regulation common to all distribution places is sufficient as the division regulation used for generating the partial key of a lot from a doubling key here, and the regulation of a proper is sufficient as it for every set of the distribution place which the regulation of a proper is sufficient as and was classified into each

distribution place on condition that a specific area and others. Also in other means, it is the same.
[0182] In addition, although some doubling keys are divided further and the key information for distribution is generated, it can replace with this, and the method enciphered with a multiplex key can also be adopted here. This modification is the same about other means to adopt the same structure.
[0183] (2) The decode server of the downstream system seen as the 2nd model [ 2nd ] of a model The partial key which received distribution through the 1st transmission network or its generating information, and the partial key which received distribution with the gestalt of a record medium or its generating information, The processing which received distribution through the 2nd transmission network and restores the cryptographic key of a proper to a key or digital data [ / based on the generating information ], The processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled, In the only output destination change of the digital data of which the processing which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, and cipher processing were canceled In the processing which decrypts the coding processing performed to the digital data concerned, and restores digital data, and the only output destination change of the restored digital data Processing which carries out scramble processing and outputs digital data is performed using the scramble key generated by the above-mentioned processing.
[0184] At this time, the output unit of a downstream system performs the processing of which the scramble processing performed to the digital data inputted from a decode server is canceled with the scramble discharge key given from the decode server, and the processing which outputs the digital data concerned with a predetermined output gestalt in the only output destination change of the digital data of which scramble processing was canceled by the above-mentioned processing.
[0185] (2-2-2) The difference between the example of a system configuration book system, and the 1st example of a distribution system The point that the partial key generation section 20 which was generated in the doubling key generation section 18 and which doubles and divides a key A1 further was added, They are the point that the write-in section 21 for writing the partial key generated in the partial key generation section 20 concerned in a record medium and the read station 38 for the reading were formed, and the point which the partial change produced in the distribution approach of key information in connection with the key information distributed having been set to three.
[0186] The partial key generation section 20 is equipment which was obtained by division processing of the doubling key generation section 18 and which doubles, divides some keys A1 by the predetermined division pattern, and generates the partial keys A11 and A12 of a lot. For example, if there are 1000 specific persons who

become a distribution place, 1000 sets of partial keys A11 and A12 will be generated. but -- not only when predetermined division patterns differ for every distribution place in this way, but all distribution places -- being the same . Moreover, you may differ for every specific area or management group.
[0187] The generated partial key is given to the distribution place management server 17 and the predetermined message distribution processing section by the partial key generation section 20. In the case of this system, the partial key generation section 20 gives the partial key A11 in the communications department which is not illustrated to distribution through a network, and gives the partial key A12 which remains to distribution by the record medium at the write-in section 21.
[0188] The write-in section 21 is equipment for writing the partial key A12 which received the notice in a predetermined record medium. The drive according to a record medium is formed in the write-in section 21. The medium of a magnetic reading method, the medium of an optical reading system, and the medium of semiconductor memory and others are used for a record medium. In addition, destination information required for distribution of a record medium is given from the distribution place management server 17. The same is said of the communications department which is not illustrated [ above-mentioned ]. However, in the case of the communications department, the address on a network is given.
[0189] In addition, a thing equipped with the drive according to the record medium which receives distribution is used for the write-in section 21 concerned and the read station 38 which makes a pair.
[0190] Moreover, although the doubling key A2 generated in the doubling key generation section 18 was distributed to the downstream system through the record medium in the 1st example of a distribution system, in the case of this 2nd example of a distribution system, the doubling key A2 is distributed through a network.
[0191] The above is the difference between the 2nd example of a distribution system, and the 1st example of a distribution system. In addition, since there is no modification in any way about a fundamental system configuration, it performs like the 1st example of a distribution system except distribution actuation of key information.
[0192] (2-2-3) the effectiveness acquired by the 2nd example of a system -- since two transmission networks (key information may be distributed when it differs on the same transmission network as the case where a different transmission network is used), and record media realize distribution of key information according to the 2nd example of a distribution system, i.e., since the distribution path of key information increases further rather than the 1st system, the malfeasance on a transmission route can offer a more difficult thing as mentioned above.
[0193] (2-3) The 3rd example of a distribution system for realizing an above-mentioned business model to the 3rd example drawing 6 of a distribution system is shown. Drawing 6 attaches and expresses the same sign with a corresponding point with drawing 4 and drawing 5 here. In addition, the 3rd example of a distribution

system corresponds to the 2nd above-mentioned means.
[0194] (2-3-1) conceptual **** -- explain the conceptual configuration of the 3rd example of a distribution system concerned first. The 1st model with which its attention was paid to distribution of digital data also in this 3rd distribution system, and the 2nd model which paid its attention to the sink side of digital data are contained.
[0195] (1) The upstream system seen as the 1st model [ 1st ] of a model The processing which generates the cryptographic key of a proper in each digital data, and the processing which enciphers digital data by the corresponding cryptographic key, The processing which generates the doubling key of the lot of a proper based on a cryptographic key at each specific person who is a distribution place, The generated processing which doubles and generates further two or more partial keys about a part of key or its generating information, The processing which distributes the part or its generating information on the generated partial key to each specific person through a transmission network, Processing written in the 1st record medium only for [ a remaining partial key or its generating information / object / for the distribution in the gestalt of a record medium ] keys, Processing which records on the remaining doubling keys which were not used for generation of a partial key or the 2nd record medium only for [ the generating information / object / for the distribution in the gestalt of a record medium ] keys, and processing which distributes the digital data with which cipher processing was performed according to the distribution schedule are performed.
[0196] The partial key with which the downstream system received distribution through the 1st transmission network on the other hand, or its generating information, The remaining partial keys which received distribution with the gestalt of a record medium or the generating information of those, and the processing which received distribution with the gestalt of the 2nd record medium, and restores the cryptographic key of a proper to a key or digital data [ / based on the generating information ], Processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled is performed.
[0197] (2) The decode server of the downstream system seen as the 2nd model [ 2nd ] of a model The partial key which received distribution through the 1st transmission network or its generating information, and the remaining partial keys which received distribution with the gestalt of the 2nd record medium or generating information of those, The processing which received distribution with the gestalt of a record medium and restores the cryptographic key of a proper to a key or digital data [ / based on the generating information ], The processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled, In the only output destination change of the digital data of which the processing which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, and cipher

processing were canceled In the processing which decrypts the coding processing performed to the digital data concerned, and restores digital data, and the only output destination change of the restored digital data Processing which carries out scramble processing and outputs digital data is performed using the scramble key generated by the above-mentioned processing.

[0198] At this time, the output unit of a downstream system performs the processing of which the scramble processing performed to the digital data inputted from a decode server is canceled with the scramble discharge key given from the decode server, and the processing which outputs the digital data concerned with a predetermined output gestalt in the only output destination change of the digital data of which scramble processing was canceled by the above-mentioned processing.

[0199] (2-3-2) The difference from the upstream system and the 2nd example of a distribution system in the example of a system configuration book system is the point of distribution of the doubling key A2 not being performed through a network, but realizing through a record medium like the 1st example of a distribution system. For this reason, about the distribution path of the doubling key A2, the same thing as the 1st example of a distribution system is used.

[0200] The above is the difference between the 3rd distribution system and the example of a distribution system mentioned above. In addition, since there is no modification in any way about a fundamental system configuration, it is the same as that of the 1st distribution system or the 2nd distribution system except distribution actuation of key information.

[0201] (2-3-3) the effectiveness acquired by the 3rd example of a distribution system -- as mentioned above, since one transmission network and two record media realize distribution of key information according to the 3rd example of a distribution system (i.e., since the distribution path by the record medium increases rather than the 2nd example of a distribution system), the thing to a malfeasance which has high safety can be offered rather than it is easy to discover the theft of key information.

[0202] (2-4) The 4th example of a distribution system for realizing an above-mentioned business model to the 4th example drawing 7 of a distribution system is shown. Drawing 7 attaches and expresses the same sign with a corresponding point with drawing 4 here. In addition, the 4th example of a distribution system corresponds to the 1st above-mentioned means.

[0203] (2-4-1) conceptual **** -- explain the conceptual configuration of the 4th example of a distribution system concerned first. The 1st model with which its attention was paid to distribution of digital data also in this 4th distribution system, and the 2nd model which paid its attention to the sink side of digital data are contained.

[0204] (1) The upstream system seen as the 1st model [ 1st ] of a model The processing which generates the cryptographic key of a proper in each digital data, and the processing which enciphers digital data by the corresponding cryptographic key,

The processing which generates the doubling key of the lot of a proper based on a cryptographic key at each specific person who is a distribution place, The generated processing which doubles and distributes a part of key or its generating information to each specific person through the 1st transmission network, Generated processing which doubles and distributes the remaining part to each specific person through the 2nd transmission network among a key or its generating information, and processing which distributes the digital data with which cipher processing was performed according to the distribution schedule are performed.
[0205] On the other hand, the downstream system received distribution through the 1st transmission network, and processing of which the processing which restores the cryptographic key of a proper to digital data [ / based on a part of key or its generating information, and them which received distribution through the 2nd transmission network and the remaining part which makes a pair ], and cipher processing performed to the digital data which corresponds using the restored cryptographic key are canceled is performed.
[0206] (2) The decode server of the downstream system seen as the 2nd model [ 2nd ] of a model Distribution was received through the 1st transmission network. A part of key or its generating information The processing which restores the cryptographic key of a proper to digital data [ / based on them which received distribution through the 2nd transmission network, and the remaining part which makes a pair ], The processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled, In the only output destination change of the digital data of which the processing which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, and cipher processing were canceled In the processing which decrypts the coding processing performed to the digital data concerned, and restores digital data, and the only output destination change of the restored digital data Processing which carries out scramble processing and outputs digital data is performed using the scramble key generated in the above-mentioned processing.
[0207] At this time, the output unit of a downstream system performs the processing of which the scramble processing performed to the digital data inputted from a decode server is canceled with the scramble discharge key given from the decode server, and the processing which outputs the digital data concerned with a predetermined output gestalt in the only output destination change of the digital data of which scramble processing was canceled by the above-mentioned processing.
[0208] (2-4-2) The difference from the upstream system and the 1st example of a distribution system in the example of a system configuration book system is the point generated in the doubling key generation section 18 that double and keys A1 and A2 are distributed by each through a network.
[0209] The above is the difference between the 4th distribution system and the 1st

example of a distribution system. In addition, since there is no modification in any way about a fundamental system configuration, it is the same as that of the 1st example of a distribution system except distribution actuation of key information.
[0210] (2-4-3) the effectiveness acquired by the 4th example of a distribution system -- since both of distribution of key information realizes through a network according to the 4th example of a distribution system, i.e., since all key information can distribute through the network which was excellent in the sex instancy, time amount until distribution of digital data is started from distribution of a key can shorten sharply compared with the case where key information is distributed using a record medium, as mentioned above.
[0211] (2-5) The 5th example of a distribution system for realizing an above-mentioned business model to the 5th example drawing 8 of a distribution system is shown. Drawing 8 attaches and expresses the same sign with a corresponding point with drawing 4 here. In addition, the 5th example of a distribution system corresponds to the 1st above-mentioned means.
[0212] (2-5-1) conceptual **** -- explain the conceptual configuration of the 5th example of a distribution system concerned first. The 1st model with which its attention was paid to distribution of digital data also in this 5th distribution system, and the 2nd model which paid its attention to the sink side of digital data are contained.
[0213] (1) The upstream system seen as the 1st model [ 1st ] of a model The processing which generates the cryptographic key of a proper in each digital data, and the processing which enciphers digital data by the corresponding cryptographic key, The processing which generates the doubling key of the lot of a proper based on a cryptographic key at each specific person who is a distribution place, The generated processing which doubles and writes a part of key or its generating information in the 1st record medium only for keys for the distribution in the gestalt of a record medium, Generated processing which doubles and writes the remaining part in the 2nd record medium only for keys for the distribution in the gestalt of a record medium among a key or its generating information, and processing which distributes the digital data with which cipher processing was performed according to the distribution schedule are performed.
[0214] On the other hand, the downstream system received distribution with the gestalt of the 1st record medium, and processing which restores the cryptographic key of a proper to digital data [ / based on a part of key or its generating information, and them which received distribution with the gestalt of the 2nd record medium and the remaining part which makes a pair ], and processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled are performed.
[0215] (2) The decode server of the downstream system seen as the 2nd model [ 2nd ] of a model Distribution was received with the gestalt of the 1st record medium.

A part of key or its generating information The processing which restores the cryptographic key of a proper to digital data [ / based on them which received distribution with the gestalt of the 2nd record medium, and the remaining part which makes a pair ], The processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled, In the only output destination change of the digital data of which the processing which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, and cipher processing were canceled In the processing which decrypts the coding processing performed to the digital data concerned, and restores digital data, and the only output destination change of the restored digital data Processing which carries out scramble processing and outputs digital data is performed using the scramble key generated by the above-mentioned processing.

[0216] At this time, the output unit of a downstream system performs the processing of which the scramble processing performed to the digital data inputted from a decode server is canceled with the scramble discharge key given from the decode server, and the processing which outputs the digital data concerned with a predetermined output gestalt in the only output destination change of the digital data of which scramble processing was canceled by the above-mentioned processing.

[0217] (2-5-2) The difference from the upstream system and the 1st example of a distribution system in the example of a system configuration book system is the point generated in the doubling key generation section 18 that double and keys A1 and A2 are distributed by each through a record medium. For this reason, in this system, the write-in section 22 for writing the doubling key A1 in a record medium, and this and the read station 39 which makes a pair are newly prepared. The configuration of the write-in section 22 or a read station 39 is the same as the configuration of other write-in sections or a read station.

[0218] The above is the difference between the 5th example of a distribution system, and the 1st example of a distribution system. In addition, since there is no modification in any way about a fundamental system configuration, it is the same as that of the 1st distribution system except distribution actuation of key information.

[0219] (2-5-3) the effectiveness acquired by the 5th example of a distribution system -- as mentioned above, since both of distribution of key information is realized through a record medium according to the 5th example of a distribution system (i.e., since discovery of a theft can distribute all key information through an easy record medium), compared with the case where key information is distributed through a network, what has the more high safety to a malfeasance can be offered.

[0220] (2-6) The 6th example of a distribution system for realizing an above-mentioned business model to the 6th example drawing 9 of a distribution system is shown. Drawing 9 attaches and expresses the same sign with a corresponding point with drawing 5 here. In addition, the 6th example of a distribution system corresponds

to the 2nd above-mentioned means.
[0221] (2-6-1) conceptual **** -- explain the conceptual configuration of the 6th example of a distribution system concerned first. The 1st model with which its attention was paid to distribution of digital data also in this 6th distribution system, and the 2nd model which paid its attention to the sink side of digital data are contained.
[0222] (1) The upstream system seen as the 1st model [ 1st ] of a model The processing which generates the cryptographic key of a proper in each digital data, and the processing which enciphers digital data by the corresponding cryptographic key, The processing which generates the doubling key of the lot of a proper based on a cryptographic key at each specific person who is a distribution place, The generated processing which doubles and generates further two or more partial keys about a part of key or its generating information, The processing which distributes the part or its generating information on the generated partial key to each specific person through the 1st transmission network, The processing which distributes the partial key which remains, or its generating information to each specific person through the 2nd transmission network, Processing which distributes the remaining doubling keys which were not used for generation of a partial key or the generating information of those to each specific person through the 3rd transmission network, and processing which distributes the digital data with which cipher processing was performed according to the distribution schedule are performed. **.
[0223] The partial key with which the downstream system received distribution through the 1st transmission network on the other hand, or its generating information, The remaining partial keys which received distribution through the 2nd transmission network, or the generating information of those, Processing which received distribution through the 3rd transmission network and restores the cryptographic key of a proper to a key or digital data [ / based on the generating information ], and processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled are performed.
[0224] (2) The decode server of the downstream system seen as the 2nd model [ 2nd ] of a model The partial key which received distribution through the 1st transmission network or its generating information, and the remaining partial keys which received distribution through the 2nd transmission network or generating information of those, The processing which received distribution through the 3rd transmission network and restores the cryptographic key of a proper to a key or digital data [ / based on the generating information ], The processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled, In the only output destination change of the digital data of which the processing which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, and cipher processing were canceled In the processing which decrypts the coding

processing performed to the digital data concerned, and restores digital data, and the only output destination change of the restored digital data Processing which carries out scramble processing and outputs digital data is performed using the scramble key generated by the above-mentioned processing.
[0225] At this time, the output unit of a downstream system performs the processing of which the scramble processing performed to the digital data inputted from a decode server is canceled with the scramble discharge key given from the decode server, and the processing which outputs the digital data concerned with a predetermined output gestalt in the only output destination change of the digital data of which scramble processing was canceled by the above-mentioned processing.
[0226] (2-6-2) The difference from the upstream system and the 2nd example of a distribution system ( drawing 5 ) in the example of a system configuration book system is the point that the partial key A12 generated in the partial key generation section 20 is distributed through a network.
[0227] The above is the difference between the 6th example of a distribution system, and the 2nd example of a distribution system. In addition, since there is no modification in any way about a fundamental system configuration, it is the same as that of the 2nd distribution system except distribution actuation of key information.
[0228] (2-6-3) the effectiveness acquired by the 6th example of a distribution system -- since all three distribution of key information realizes through a network according to the 6th example of a distribution system, i.e., since all key information can distribute through the network which was excellent in the sex instancy, time amount until distribution of digital data is started from distribution of a key can shorten sharply compared with the case where key information is distributed using a record medium, as mentioned above.
[0229] Furthermore, since the number of the key information distributed is three, compared with the case where key information is distributed for two key information through a network, what has the more high safety to a malfeasance can be offered.
[0230] (2-7) The 7th example of a distribution system for realizing an above-mentioned business model to the 7th example drawing 10 of a distribution system is shown. Drawing 10 attaches and expresses the same sign with a corresponding point with drawing 6 and drawing 8 here. In addition, the 7th example of a distribution system corresponds to the 2nd above-mentioned means.
[0231] (2-7-1) conceptual **** -- explain the conceptual configuration of the 7th example of a distribution system concerned first. The 1st model with which its attention was paid to distribution of digital data also in this 7th distribution system, and the 2nd model which paid its attention to the sink side of digital data are contained.
[0232] (1) The upstream system seen as the 1st model [ 1st ] of a model The processing which generates the cryptographic key of a proper in each digital data, and the processing which enciphers digital data by the corresponding cryptographic key,

The processing which generates the doubling key of the lot of a proper based on a cryptographic key at each specific person who is a distribution place, The generated processing which doubles and generates further two or more partial keys about a part of key or its generating information, Processing written in the 1st record medium only for [ the part or its generating information on the generated partial key / object / for the distribution in the gestalt of a record medium ] keys, Processing written in the 2nd record medium only for [ a remaining partial key or its generating information / object / for the distribution in the gestalt of a record medium ] keys, Processing which records on the remaining doubling keys which were not used for generation of a partial key or the 3rd record medium only for [ the generating information / object / for the distribution in the gestalt of a record medium ] keys, and processing which distributes the digital data with which cipher processing was performed according to the distribution schedule are performed. [0233] The partial key with which the downstream system received distribution with the gestalt of the 1st record medium on the other hand, or its generating information, The remaining partial keys which received distribution with the gestalt of the 2nd record medium, or the generating information of those, Processing of which the processing which received distribution with the gestalt of the 3rd record medium, and restores the cryptographic key of a proper to a key or digital data [ / based on the generating information ], and cipher processing performed to the digital data which corresponds using the restored cryptographic key are canceled is performed.

[0234] (2) The decode server of the downstream system seen as the 2nd model [ 2nd ] of a model The partial key which received distribution with the gestalt of the 1st record medium or its generating information, and the remaining partial keys which received distribution with the gestalt of the 2nd record medium or generating information of those, The processing which received distribution with the gestalt of the 3rd record medium, and restores the cryptographic key of a proper to a key or digital data [ / based on the generating information ], The processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled, In the only output destination change of the digital data of which the processing which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, and cipher processing were canceled In the processing which decrypts the coding processing performed to the digital data concerned, and restores digital data, and the only output destination change of the restored digital data Processing which carries out scramble processing and outputs digital data is performed using the scramble key generated by the above-mentioned processing.

[0235] At this time, the output unit of a downstream system performs the processing of which the scramble processing performed to the digital data inputted from a decode server is canceled with the scramble discharge key given from the decode server, and the processing which outputs the digital data concerned with a

predetermined output gestalt in the only output destination change of the digital data of which scramble processing was canceled by the above-mentioned processing.
[0236] (2-7-2) The difference from the upstream system and the 3rd example of a distribution system in the example of a system configuration book system is the point that the partial keys A11 and A12 generated in the partial key generation section 20 are distributed by each through a record medium. For this reason, in this example of a system, the write-in section 22 for writing the partial key A11 in a record medium, and this and the read station 39 which makes a pair are newly prepared. The configuration of the write-in section 22 or a read station 39 is the same as the configuration of other write-in sections or a read station.
[0237] The above is the difference between the 7th example of a distribution system, and the 3rd example of a distribution system. In addition, since there is no modification in any way about a fundamental system configuration, it is the same as that of the 3rd distribution system except distribution actuation of key information.
[0238] (2-7-3) the effectiveness acquired by the 7th example of a distribution system -- since all three distribution of key information is realized through a record medium according to the 7th example of a distribution system (i.e., since discovery of a theft can distribute all key information through an easy record medium), compared with the case where the path which distributes key information through a network is included, what has the more high safety to a malfeasance can offer as mentioned above.
[0239] (2-8) The 8th example of a distribution system for realizing an above-mentioned business model to the 8th example drawing 11 of a distribution system is shown. Drawing 11 attaches and expresses the same sign with a corresponding point with drawing 4 here. the example of a system concerned -- the 1- to the above-mentioned -- unlike the 7th example of a distribution system, the cryptographic key of digital data is not divided but the cryptographic key concerned is enciphered with another multiplex key of a proper for every distribution place. That is, the 8th example of a distribution system corresponds to the 3rd above-mentioned means.
[0240] (2-8-1) conceptual **** -- explain the conceptual configuration of the 8th example of a distribution system concerned first. The 1st model with which its attention was paid to distribution of digital data also in this 8th distribution system, and the 2nd model which paid its attention to the sink side of digital data are contained.
[0241] (1) The upstream system seen as the 1st model [ 1st ] of a model The processing which generates the 1st cryptographic key of a proper in each digital data, and the processing which enciphers digital data by the 1st cryptographic key, The processing which is the 2nd cryptographic key of a proper and generates the thing of a proper at digital data to each specific person who is a distribution place, The processing which enciphers the 1st cryptographic key or its generating information, and is distributed to a specific person through a transmission network by the 2nd cryptographic key, Processing written in the record medium only for [ the 2nd

cryptographic key / object / for the distribution in the gestalt of a record medium ] keys and processing which distributes the digital data with which cipher processing was performed according to the distribution schedule are performed.
[0242] A downstream system cancels cipher processing performed to the 1st cryptographic key which received distribution through the transmission network based on the 2nd cryptographic key which received distribution with the gestalt of a record medium on the other hand, or its generating information, or its generating information, and performs the processing which restores the cryptographic key of a proper to corresponding digital data, and processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled.
[0243] (2) The decode server of the downstream system seen as the 2nd model [ 2nd ] of a model Cipher processing performed to the 1st cryptographic key which received distribution through the transmission network based on the 2nd cryptographic key which received distribution, or its generating information with the gestalt of a record medium, or its generating information is canceled. The processing which restores the cryptographic key of a proper to corresponding digital data, and the processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled, In the only output destination change of the digital data of which the processing which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, and cipher processing were canceled In the processing which decrypts the coding processing performed to the digital data concerned, and restores digital data, and the only output destination change of the restored digital data Processing which carries out scramble processing and outputs digital data is performed using the scramble key generated by the above-mentioned processing.
[0244] At this time, the output unit of a downstream system performs the processing of which the scramble processing performed to the digital data inputted from a decode server is canceled with the scramble discharge key given from the decode server, and the processing which outputs the digital data concerned with a predetermined output gestalt in the only output destination change of the digital data of which scramble processing was canceled by the above-mentioned processing.
[0245] (2-8-2) a system configuration -- the 1- of the above-mentioned [ the 8th example of a distribution system ] as mentioned above -- differ in base example [ 7th / of distribution system ] mode of processing. For this reason, the multiplex key generation section 23 which generates the multiplex key B of a proper at a distribution place in the 8th example of a distribution system, The key encryption processing section 24 which enciphers a cryptographic key A with the multiplex key B concerned, The write-in section 25 used for writing the multiplex key B in a record medium, and distributing it and the read station 40 which makes this and a pair are replaced and used for the doubling key generation section 18 in the 1st example of a

distribution system, the write-in section 19, and a read station 32.
[0246] The multiplex key generation section 23 is equipment which generates the cryptographic key B of a proper for every distribution place to the cryptographic key A generated for every contents. For example, if there are 1000 specific persons who become a distribution place, 1000 kinds of multiplex keys B will be generated. In addition, the multiplex key B may generate and use a different multiplex key B for every contents, if the distribution place is the same and there is also an approach using the always same multiplex key. From a viewpoint of safety, the latter is desirable. Moreover, a different key for every specific area or management group may be used.
[0247] The key encryption processing section 24 is equipment which enciphers a cryptographic key using the multiplex key of a proper for every distribution place. The cryptographic key enciphered in the key encryption processing section 24 is distributed to the downstream system which corresponds through a network from the non-illustrated communications department.
[0248] The configuration of the write-in section 25 and a read station 40 is the same as the above-mentioned write-in section and a read station. But being written by reading and the write-in section 25 and the read station 40 differs from the above-mentioned example of a distribution system at the point which is a multiplex key.
[0249] (2-8-3) Explain briefly only a different part from the example of a distribution system of [ 1st ] the distribution actuation of the digital data in the example of a distribution system of the distribution actuation 8th of digital data. That is, although the cryptographic key concerned was doubled, and it gave the key generation section 18, it doubled with it and the key was generated in the 1st example of a distribution system when the cryptographic key A of a proper was generated to contents, in the case of this example of a system, a cryptographic key A is enciphered using the multiplex key B of the proper generated for every distribution place, and it distributes to a downstream system through a network. Moreover, the multiplex key B used for encryption of the cryptographic key A concerned is addressed to the distribution person who corresponds, respectively, and it distributes with the gestalt of a record medium.
[0250] In addition, the generated multiplex key B is managed by the distribution place management server 17. The above processing actuation is a primary difference with the 1st system.
[0251] (2-8-4) the effectiveness acquired by the 8th example of a distribution system -- as mentioned above according to the 8th example of a distribution system By having carried out to two, the cryptographic key A which had the key information distributed to the specific person who manages a downstream system enciphered, and the multiplex key B, and having considered as the configuration which distributes them through two or more paths Even if the theft of one of the key information is carried out, unless the theft also of another side will be carried out, the distribution

model which can prevent the outflow of a cryptographic key can be offered.
[0252] And since it distributes with the gestalt of the record medium which is easy to discover a theft about a multiplex key, when it becomes clear that the theft of the multiplex key was carried out by the malfeasance, it can stop distributing the enciphered cryptographic key A which is performed through a network, and the safety to a malfeasance can be maintained by resuming from the procedure which distributes another multiplex key B as a record medium.
[0253] Of course, since the downstream structure of a system is the same as the 1st example of a distribution system, excelling also in the economical efficiency for employment is the same as that of the 1st example of a distribution system.
[0254] (2-9) The 9th example of a system for realizing an above-mentioned business model to the 9th example drawing 12 of a distribution system is shown. Drawing 12 attaches and expresses the same sign with a corresponding point with drawing 11 here. In addition, the 9th example of a distribution system corresponds to the 4th above-mentioned means.
[0255] (2-9-1) conceptual **** -- explain the conceptual configuration of the 9th example of a distribution system concerned first. The 1st model with which its attention was paid to distribution of digital data also in this 9th distribution system, and the 2nd model which paid its attention to the sink side of digital data are contained.
[0256] The processing whose upstream system seen as the 1st model generates the 1st cryptographic key of a proper in each digital data, The processing which enciphers digital data by the 1st cryptographic key, and the processing which is the 2nd cryptographic key of a proper and generates the thing of a proper at digital data to each specific person who is a distribution place, The processing which enciphers the 1st cryptographic key or its generating information, and is distributed to a specific person through the 1st transmission network by the 2nd cryptographic key of the above, The processing which generates the doubling key of the lot of a proper based on the 2nd cryptographic key at each specific person who is a distribution place, The generated processing which doubles and distributes the part or its generating information on a key to each specific person through the 2nd transmission network, Generated processing which doubles and writes the remaining part or its generating information on a key in the record medium only for keys for the distribution in the gestalt of a record medium, and processing which distributes the digital data with which cipher processing was performed according to the distribution schedule are performed.
[0257] On the other hand, the downstream system received distribution through the 2nd transmission network. Some keys Received distribution through the record medium and the 2nd cryptographic key is restored from the remaining part of a key. The processing which cancels cipher processing performed to the 1st cryptographic key which received distribution through the 1st transmission network, or its

generating information, and restores the cryptographic key of a proper to corresponding digital data, Processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled is performed.

[0258] (2) The decode server of the downstream system seen as the 2nd model [ 2nd ] of a model Received distribution through the 2nd transmission network, received distribution through some keys and a record medium, and the 2nd cryptographic key is restored from the remaining part of a key. The processing which cancels cipher processing performed to the 1st cryptographic key which received distribution through the 1st transmission network, or its generating information, and restores the cryptographic key of a proper to corresponding digital data, The processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled, In the only output destination change of the digital data of which the processing which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, and cipher processing were canceled In the processing which decrypts the coding processing performed to the digital data concerned, and restores digital data, and the only output destination change of the restored digital data Processing which carries out scramble processing and outputs digital data is performed using the scramble key generated by the above-mentioned processing.

[0259] At this time, the output unit of a downstream system performs the processing of which the scramble processing performed to the digital data inputted from a decode server is canceled with the scramble discharge key given from the decode server, and the processing which outputs the digital data concerned with a predetermined output gestalt in the only output destination change of the digital data of which scramble processing was canceled by the above-mentioned processing.

[0260] (2-9-2) The difference between the example of a system configuration book system, and the 8th example of a distribution system The point that divided the multiplex key B generated in the multiplex key generation section 23, and the doubling key generation section 26 which generates the doubling key B1 and B-2 of a lot was added, it was generated in the doubling key generation section 26 concerned -- doubling -- some keys -- it is the point that the write-in section 27 for writing B-2 in a record medium and the read station 41 for the reading were formed.

[0261] The doubling key generation section 26 is equipment which divides the multiplex key B generated for every distribution place by the division pattern of a proper for every distribution place, and generates the doubling key B1 and B-2 of a lot. It is also possible to use a division regulation common about all distribution places, and the division regulation of the doubling key generation section 26 is possible also for assigning the division regulation of a proper for every distribution place, and can also change these division regulation per contents. Moreover, a commuter's ticket or

changing irregularly are also possible also during distribution of contents. Moreover, it is also possible to assign a different division regulation for every specific area or management group.

[0262] The configuration of the write-in section 27 and a read station 41 is the same as other write-in sections or a read station. In addition, since there is no modification in any way about a fundamental system configuration, it is the same as that of the 8th example of a distribution system except distribution actuation of key information.

[0263] (2-9-3) According to the 9th example of a distribution system, divide the multiplex key B into the doubling key B1 and B-2 of a lot as mentioned above. the effectiveness acquired by the 9th example of a distribution system -- in a network one side Since the configuration which distributes another side with a record medium is adopted, in addition to distributing what sent and divided the multiplex key B itself, compared with the 8th example of a distribution system, what has the more high safety to a malfeasance can be offered by increasing a distribution path from two to three.

[0264] (2-10) The 10th example of a distribution system for realizing an above-mentioned business model to the 10th example drawing 13 of a distribution system is shown. Drawing 13 attaches and expresses the same sign with a corresponding point with drawing 12 here. In addition, the 10th example of a distribution system corresponds to the 4th above-mentioned means.

[0265] (2-10-1) conceptual **** -- explain the conceptual configuration of the 10th example of a distribution system concerned first. The 1st model which paid its attention to distribution of digital data, and the 2nd model which paid its attention to the sink side of digital data are contained in this 10th distribution system.

[0266] (1) The upstream system seen as the 1st model [ 1st ] of a model The processing which generates the 1st cryptographic key of a proper in each digital data, and the processing which enciphers digital data by the 1st cryptographic key, The processing which is the 2nd cryptographic key of a proper and generates the thing of a proper at digital data to each specific person who is a distribution place, The processing which writes the 1st cryptographic key enciphered by the 2nd cryptographic key or its generating information in the 1st record medium only for keys for the distribution in the gestalt of a record medium, The processing which generates the doubling key of the lot of a proper based on the 2nd cryptographic key at each specific person who is a distribution place, The generated processing which doubles and distributes the part or its generating information on a key to each specific person through a transmission network, Generated processing which doubles and writes the remaining part or its generating information on a key in the 2nd record medium only for keys for the distribution in the gestalt of a record medium, and processing which distributes the digital data with which cipher processing was performed according to the distribution schedule are performed.

[0267] On the other hand, the downstream system received distribution through the

transmission network. Some keys Received distribution through the 2nd record medium and the 2nd cryptographic key is restored from the remaining part of a key. The processing which cancels cipher processing performed to the 1st cryptographic key which received distribution through the 1st record medium, or its generating information, and restores the cryptographic key of a proper to corresponding digital data, Processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled is performed.
[0268] (2) The decode server of the downstream system seen as the 2nd model [ 2nd ] of a model Received distribution through the transmission network, received distribution through some keys and the 2nd record medium, and the 2nd cryptographic key is restored from the remaining part of a key. The processing which cancels cipher processing performed to the 1st cryptographic key which received distribution through the 1st record medium, or its generating information, and restores the cryptographic key of a proper to corresponding digital data, The processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled, The processing which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, In the processing which decrypts the coding processing which is the only output destination change of the digital data of which cipher processing was canceled, and is performed to the digital data concerned, and restores digital data, and the only output destination change of the restored digital data Processing which carries out scramble processing and outputs digital data is performed using the scramble key generated by the above-mentioned processing.
[0269] At this time, the output unit of a downstream system performs the processing of which the scramble processing performed to the digital data inputted from a decode server is canceled with the scramble discharge key given from the decode server, and the processing which outputs the digital data concerned with a predetermined output gestalt in the only output destination change of the digital data of which scramble processing was canceled by the above-mentioned processing.
[0270] (2-10-2) The difference between the example of a system configuration book system and the 9th example of a distribution system is the point of not performing distribution of the enciphered cryptographic key A through a network, but carrying out through a record medium. For this reason, in the case of this example of a system, it differs in that the write-in section 28 and a read station 42 are newly formed. Since it is the same as other write-in sections or a read station, the configuration of the write-in section 28 and a read station 42 is omitted.
[0271] In addition, since there is no modification in any way about a fundamental system configuration, it is the same as that of the 8th example of a distribution system except distribution actuation of key information.
[0272] (2-10-3) the effectiveness acquired by the 10th example of a distribution system -- as mentioned above, according to the 10th example of a distribution

system, as compared with the case where the part to which the enciphered cryptographic key A is distributed through a record medium, and the key concerned are distributed through a network, the early detection of a theft becomes possible, and the effectiveness of being easy to take cures, such as modification of a cryptographic key, can be expected.

[0273] (2-11) The 11th example of a distribution system for realizing an above-mentioned business model to the 11th example drawing 14 of a distribution system is shown. Drawing 14 attaches and expresses the same sign with a corresponding point with drawing 11 here. In addition, the 11th example of a distribution system corresponds to the 3rd above-mentioned means.

[0274] (2-11-1) conceptual **** -- explain the conceptual configuration of the 11th example of a distribution system concerned first. The 1st model which paid its attention to distribution of digital data, and the 2nd model which paid its attention to the sink side of digital data are contained in this 11th distribution system.

[0275] (1) The upstream system seen as the 1st model [ 1st ] of a model The processing which generates the 1st cryptographic key of a proper in each digital data, and the processing which enciphers digital data by the 1st cryptographic key, The processing which is the 2nd cryptographic key of a proper and generates the thing of a proper at digital data to each specific person who is a distribution place, The processing which enciphers the 1st cryptographic key or its generating information, and is distributed to a specific person through the 1st transmission network by the 2nd cryptographic key, Processing which distributes the 2nd cryptographic key to a specific person through the 2nd transmission network, and processing which distributes the digital data with which cipher processing was performed according to the distribution schedule are performed.

[0276] The processing of which the processing by which the cryptographic key of a proper restores to the digital data which cancels cipher processing performed to the 1st cryptographic key which received distribution through the 1st transmission network on the other hand based on the 2nd cryptographic key in which the downstream system received distribution through the 2nd transmission network, or its generating information, or its generating information, and corresponds, and cipher processing which are performed to the digital data which corresponds using the restored cryptographic key cancel performs.

[0277] (2) The decode server of the downstream system seen as the 2nd model [ 2nd ] of a model Based on the 2nd cryptographic key which received distribution through the 2nd transmission network, or its generating information The processing which cancels cipher processing performed to the 1st cryptographic key which received distribution through the 1st transmission network, or its generating information, and restores the cryptographic key of a proper to corresponding digital data, The processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled, In the only output

destination change of the digital data of which the processing which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, and cipher processing were canceled In the processing which decrypts the coding processing performed to the digital data concerned, and restores digital data, and the only output destination change of the restored digital data Processing which carries out scramble processing and outputs digital data is performed using the scramble key generated by the above-mentioned processing.

[0278] At this time, the output unit of a downstream system performs the processing of which the scramble processing performed to the digital data inputted from a decode server is canceled with the scramble discharge key given from the decode server, and the processing which outputs the digital data concerned with a predetermined output gestalt in the only output destination change of the digital data of which scramble processing was canceled by the above-mentioned processing.

[0279] (2-11-2) The difference between the example of a system configuration book system and the 8th example of a distribution system is the point of not performing the multiplex key B through a record medium, but carrying out through a network. Except it, since it is the same as the 8th example of a distribution system, it is the same as that of the 8th example of a distribution system except distribution actuation of key information. But it is desirable to encipher and distribute with the public key which the distribution place exhibits, after checking the other party's justification by a digital certificate etc. on the occasion of distribution of the multiplex key B.

[0280] (2-11-3) the effectiveness acquired by the 11th example of a distribution system -- since the technique of distributing the multiplex key B through a network is adopted as mentioned above according to the 11th example of a distribution system, time amount until distribution of digital data is started from distribution of a key can be shortened sharply.

[0281] (2-12) The 12th example of a distribution system for realizing an above-mentioned business model to the 12th example drawing 15 of a distribution system is shown. Drawing 15 attaches and expresses the same sign with a corresponding point with drawing 11 and drawing 13 here. In addition, the 12th example of a distribution system corresponds to the 3rd above-mentioned means.

[0282] (2-12-1) conceptual **** -- explain the conceptual configuration of the 12th example of a distribution system concerned first. The 1st model which paid its attention to distribution of digital data, and the 2nd model which paid its attention to the sink side of digital data are contained in this 12th distribution system.

[0283] (1) The upstream system seen as the 1st model [ 1st ] of a model The processing which generates the 1st cryptographic key of a proper in each digital data, and the processing which enciphers digital data by the 1st cryptographic key, The processing which is the 2nd cryptographic key of a proper and generates the thing of a proper at digital data to each specific person who is a distribution place, The

processing which enciphers the 1st cryptographic key or its generating information, and is written in the 1st record medium only for keys for the distribution in the gestalt of a record medium by the 2nd cryptographic key, Processing written in the 2nd record medium only for [ the 2nd cryptographic key / object / for the distribution in the gestalt of a record medium ] keys and processing which distributes the digital data with which cipher processing was performed according to the distribution schedule are performed.

[0284] The processing of which cipher processing performed to the 1st cryptographic key which received distribution with the gestalt of the 1st record medium based on the 2nd cryptographic key in which the downstream system received distribution with the gestalt of the 2nd record medium on the other hand, or its generating information, or its generating information is canceled, and the processing which restores the cryptographic key of a proper to corresponding digital data, and cipher processing performed to the digital data which corresponds using the restored cryptographic key are canceled performs.

[0285] (2) The decode server of the downstream system seen as the 2nd model [ 2nd ] of a model Based on the 2nd cryptographic key which received distribution with the gestalt of the 2nd record medium, or its generating information The processing which cancels cipher processing performed to the 1st cryptographic key which received distribution with the gestalt of the 1st record medium, or its generating information, and restores the cryptographic key of a proper to corresponding digital data, The processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled, In the only output destination change of the digital data of which the processing which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, and cipher processing were canceled In the processing which decrypts the coding processing performed to the digital data concerned, and restores digital data, and the only output destination change of the restored digital data Processing which carries out scramble processing and outputs digital data is performed using the scramble key generated by the above-mentioned processing.

[0286] At this time, the output unit of a downstream system performs the processing of which the scramble processing performed to the digital data inputted from a decode server is canceled with the scramble discharge key given from the decode server, and the processing which outputs the digital data concerned with a predetermined output gestalt in the only output destination change of the digital data of which scramble processing was canceled by the above-mentioned processing.

[0287] (2-12-2) The difference between the example of a system configuration book system and the 8th example of a distribution system is the point of not performing distribution of the enciphered cryptographic key A through a network, but carrying out through a record medium. Except it, since it is the same as the 8th example of a

distribution system, it is the same as that of the 8th example of a distribution system except distribution actuation of key information.
[0288] (2-12-3) the effectiveness acquired by the 12th example of a distribution system -- as mentioned above, since both of distribution of key information is realized through a record medium according to the 12th example of a distribution system (i.e., since discovery of a theft can distribute all key information through an easy record medium), compared with the case where key information is distributed through a network, what has the more high safety to a malfeasance can be offered.
[0289] (2-13) The 13th example of a distribution system for realizing an above-mentioned business model to the 13th example drawing 16 of a distribution system is shown. Drawing 16 attaches and expresses the same sign with a corresponding point with drawing 12 here. In addition, the 13th example of a distribution system corresponds to the 4th above-mentioned means.
[0290] (2-13-1) conceptual **** -- explain the conceptual configuration of the 13th example of a distribution system concerned first. The 1st model which paid its attention to distribution of digital data, and the 2nd model which paid its attention to the sink side of digital data are contained in this 13th distribution system.
[0291] (1) The upstream system seen as the 1st model [ 1st ] of a model The processing which generates the 1st cryptographic key of a proper in each digital data at somewhere in a system, The processing which enciphers digital data by the 1st cryptographic key, and the processing which is the 2nd cryptographic key of a proper and generates the thing of a proper at digital data to each specific person who is a distribution place, The processing which enciphers the 1st cryptographic key or its generating information, and is distributed to a specific person through the 1st transmission network by the 2nd cryptographic key, The processing which generates the doubling key of the lot of a proper based on the 2nd cryptographic key at each specific person who is a distribution place, The generated processing which doubles and distributes the part or its generating information on a key to each specific person through the 2nd transmission network, Generated processing which doubles and distributes the remaining part or its generating information on a key to each specific person through the 3rd transmission network, and processing which distributes the digital data with which cipher processing was performed according to the distribution schedule are performed.
[0292] On the other hand, the downstream system received distribution through the 2nd transmission network. Some keys Received distribution through the 3rd transmission network and the 2nd cryptographic key is restored from the remaining part of a key. The processing which cancels cipher processing performed to the 1st cryptographic key which received distribution through the 1st transmission network, or its generating information, and restores the cryptographic key of a proper to corresponding digital data, Processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled is

performed.
[0293] (2) The decode server of the downstream system seen as the 2nd model [ 2nd ] of a model Received distribution through the 2nd transmission network, received distribution through some keys and the 3rd transmission network, and the 2nd cryptographic key is restored from the remaining part of a key. The processing which cancels cipher processing performed to the 1st cryptographic key which received distribution through the 1st transmission network, or its generating information, and restores the cryptographic key of a proper to corresponding digital data, The processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled, In the only output destination change of the digital data of which the processing which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, and cipher processing were canceled In the processing which decrypts the coding processing performed to the digital data concerned, and restores digital data, and the only output destination change of the restored digital data Processing which carries out scramble processing and outputs digital data is performed using the scramble key generated by the above-mentioned processing.
[0294] At this time, the output unit of a downstream system performs the processing of which the scramble processing performed to the digital data inputted from a decode server is canceled with the scramble discharge key given from the decode server, and the processing which outputs the digital data concerned with a predetermined output gestalt in the only output destination change of the digital data of which scramble processing was canceled by the above-mentioned processing.
[0295] (2-13-2) The difference between the example of a system configuration book system and the 9th example of a distribution system is the point of having generated from the multiplex key B, and not using a record medium for distribution of key B-2, but carrying out through a network. Namely, it differs in that distribution of three key information is altogether performed through a network. Except it, since it is the same as the 9th example of a distribution system, it is the same as that of the 9th example of a distribution system except distribution actuation of key information.
[0296] (2-13-3) the effectiveness acquired by the 13th example of a distribution system -- since all three distribution of key information is performed through a network as mentioned above according to the 13th example of a distribution system, compared with the case where key information is distributed using a record medium, time amount until distribution of digital data is started from distribution of a key can be shortened sharply.
[0297] Furthermore, since the number of the key information distributed is three, compared with the case where key information is distributed for two key information through a network, what has the more high safety to a malfeasance can be offered.
[0298] (2-14) The 14th example of a distribution system for realizing an above-

mentioned business model to the 14th example drawing 17 of a system is shown. Drawing 17 attaches and expresses the same sign with a corresponding point with drawing 13 here. In addition, the 14th example of a distribution system corresponds to the 4th above-mentioned means.
[0299] (2-14-1) conceptual **** -- explain the conceptual configuration of the 14th example of a distribution system concerned first. The 1st model which paid its attention to distribution of digital data, and the 2nd model which paid its attention to the sink side of digital data are contained in this 14th distribution system.
[0300] (1) The upstream system seen as the 1st model [ 1st ] of a model The processing which generates the 1st cryptographic key of a proper in each digital data, and the processing which enciphers digital data by the 1st cryptographic key, The processing which is the 2nd cryptographic key of a proper and generates the thing of a proper at digital data to each specific person who is a distribution place, The processing which writes the 1st cryptographic key enciphered by the 2nd cryptographic key or its generating information in the 1st record medium only for keys for the distribution in the gestalt of a record medium, The processing which generates the doubling key of the lot of a proper based on the 2nd cryptographic key at each specific person who is a distribution place, The generated processing which doubles and writes the part or its generating information on a key in the 2nd record medium only for keys for the distribution in the gestalt of a record medium, Generated processing which doubles and writes the remaining part or its generating information on a key in the 3rd record medium only for keys for the distribution in the gestalt of a record medium, and processing which distributes the digital data with which cipher processing was performed according to the distribution schedule are performed.
[0301] On the other hand, the downstream system received distribution through the 2nd record medium. Some keys Received distribution through the 3rd record medium and the 2nd cryptographic key is restored from the remaining part of a key. The processing which cancels cipher processing performed to the 1st cryptographic key which received distribution through the 1st record medium, or its generating information, and restores the cryptographic key of a proper to corresponding digital data, Processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled is performed.
[0302] (2) The decode server of the downstream system seen as the 2nd model [ 2nd ] of a model Received distribution through the 2nd record medium, received distribution through some keys and the 3rd record medium, and the 2nd cryptographic key is restored from the remaining part of a key. The processing which cancels cipher processing performed to the 1st cryptographic key which received distribution through the 1st record medium, or its generating information, and restores the cryptographic key of a proper to corresponding digital data, The processing of which cipher processing performed to the digital data which corresponds using the restored cryptographic key is canceled, In the only output destination change of the digital

data of which the processing which generates a scramble key and its discharge key locally on condition that the playback conditions attached to digital data are fulfilled, and cipher processing were canceled In the processing which decrypts the coding processing performed to the digital data concerned, and restores digital data, and the only output destination change of the restored digital data Processing which carries out scramble processing and outputs digital data is performed using the scramble key generated by the above-mentioned processing.

[0303] At this time, the output unit of a downstream system performs the processing of which the scramble processing performed to the digital data inputted from a decode server is canceled with the scramble discharge key given from the decode server, and the processing which outputs the digital data concerned with a predetermined output gestalt in the only output destination change of the digital data of which scramble processing was canceled by the above-mentioned processing.

[0304] (2-14-2) The difference between the example of a system configuration book system and the 10th example of a distribution system is the point of having generated from the multiplex key B, and not using a network for distribution of a key B1, but carrying out through a record medium. Namely, it differs in that distribution of three key information is altogether performed through a record medium. For this reason, in the case of this example of a system, the write-in section 29 and a read station 43 are newly formed. Since it is the same as other write-in sections or a read station, the configuration of the write-in section 29 and a read station 43 is omitted.

[0305] Except it, since it is the same as the 10th example of a distribution system, it is the same as that of the 10th example of a distribution system except distribution actuation of key information.

[0306] (2-14-3) the effectiveness acquired by the 14th example of a distribution system -- as mentioned above, since all three distribution of key information is performed through a record medium according to the 14th example of a distribution system (i.e., since discovery of a theft can distribute all key information through an easy record medium), compared with the case where the path which distributes key information through a network is included, what has the more high safety to a malfeasance can offer.

[0307] (3) employment gestalt the 1- assumed in each example of a system -- in the 14th example of a distribution system Any of the function part which constitutes an upstream system are performed within the system of the right person 1 of distribution. or [ that any are performed within the electronic distribution entrepreneur's 2 system ], although the viewpoint of the technical effectiveness accepted from the system configuration concerned explained, without considering as a problem (without making into a problem whether to be carried out by the either when an upstream system is employed by three or more persons) Here, it explains what kind of difference arises in the effectiveness on business about the employment gestalt assumed.

[0308] The safety of the upstream system seen from the right person of distribution is explained especially here. It cannot be overemphasized that priority may be given to the safety which the right person of distribution of contents was for thinking that a malfeasance receives damage in many cases, but looked at this from other entrepreneurs depending on the business model.
[0309] Drawing 18 is summarized from a viewpoint of how the contents coding section 12, the encryption section 13, and the key generating section 16 (indirectly the doubling key generation section (partial key generation section) and the multiplex key generation section (the doubling key generation section)) are arranged among the function parts which constitute an upstream system. However, the case where the number of the key information distributed is two is shown by drawing 18 . When three or more kinds of key information is distributed, the part "one [ part ]" was written by drawing 18 means "at least one."
[0310] (3-1) the employment gestalt of the 1st employment gestalt 1st -- both the generating person of a cryptographic key A the executor of coding processing and the executor of cipher processing -- although -- it is the case where he is a right person of distribution (namely, when the contents coding section 12, the encryption section 13, and the key generating section 16 are formed in the system side of the right person of distribution), and consider the case where the right person of distribution also performs distribution of key information.
[0311] Here, generating of key information assumes the case where the right person of distribution who is a distribution subject carries out. That is, the case where the right person of distribution also performs the doubling key generation section 18 (the partial key generation section 20 is also included depending on the example of a system.), the multiplex key generation section 23, and the key encryption processing section 24 (the doubling key generation section 26 is also included depending on the example of a system.) is assumed.
[0312] In this case, the electronic distribution entrepreneur's 2 system will perform only business which distributes the digital data with which cipher processing was performed to a specific person. That is, only the sending-out server 14 will belong to the electronic distribution entrepreneur's 2 system.
[0313] If such an employment gestalt is taken, the person in the position in which the cryptographic key (master key) used for encryption of digital data can be known can do it only with the right person 1 of distribution. Since this does not need to take into consideration any danger that a cryptographic key will flow out outside through the electronic distribution entrepreneur 2 from the viewpoint of the right person 1 of distribution, it has the advantage that contents can be offered in comfort.
[0314] (3-2) Consider fundamentally the case where the distribution subject of key information becomes the bottom of the 1st employment gestalt with the right person 1 of distribution, and two persons of the electronic distribution entrepreneur 2, with the employment gestalt of the 2nd employment gestalt 2nd.

[0315] For example, although it doubles in the 2nd example of a distribution system ( drawing 5 ) and the right person 1 of distribution performs generation and distribution of a key A2, the case where the electronic distribution entrepreneur 2 performs distribution of the processing which generates the partial keys A11 and A12 from the doubling key A1, and the generated partial key can be considered. In addition, when the same, the 3rd example of a distribution system ( drawing 6 ), the 6th example of a distribution system ( drawing 9 ), and the 7th example of a distribution system ( drawing 10 ) can be considered.
[0316] Moreover, for example, also when [ which was generated ] doubling and making the electronic distribution entrepreneur 2 perform only writing to the record medium of a key or a partial key, and distribution, it thinks. In this case, the 1st example of a distribution system ( drawing 4 ), the 2nd example of a distribution system ( drawing 5 ), The 3rd example of a distribution system (when reaching partial key A12 in drawing 6 or writing in the doubling key A2), The 5th example of a distribution system (when doubling by drawing 8 and writing in a key A1 or A2), The 7th example of a distribution system (when writing in any one key information or any two key information by drawing 10 ), The 9th example of a distribution system, the 10th example of a distribution system (when doubling by drawing 12 and writing in key B-2) (when writing in the cryptographic key or doubling key B-2 enciphered by drawing 13 ), There are the 12th example of a distribution system (when writing in the cryptographic key enciphered by drawing 15 ) and the 14th example of a distribution system (when writing in any one key information or any two key information by drawing 17 ).
[0317] Since the person in the position in which the cryptographic key (master key) used for encryption of digital data also as such an employment gestalt can be known turns into only a right person of distribution of contents, he can do it with an employment gestalt safe for the right person of distribution.
[0318] In addition, although the right person 1 of distribution performs encryption and distribution of a cryptographic key A to what can secure safety as compared with the existing distribution model although dependability falls a little compared with the above thing in the 9th example of a distribution system ( drawing 12 ), the case to which it doubles and the electronic distribution entrepreneur 2 carries out distribution of a key where it is generated with generation of the doubling key B1 of the multiplex key B and B-2 can be considered.
[0319] The 10th example of a distribution system ( drawing 13 ), the 12th example of a distribution system ( drawing 15 ), the 13th example of a distribution system ( drawing 16 ), and the 14th example of a distribution system ( drawing 17 ) can be considered to the same thing as this.
[0320] (3-3) Consider fundamentally the case where the distribution subject of key information becomes the bottom of the 1st employment gestalt with the electronic distribution entrepreneur 2, with the employment gestalt of the 3rd employment

gestalt 3rd.
[0321] For example, in the 1st example of a distribution system ( drawing 4 ), although the right person of distribution performs generating of a cryptographic key, the case where the electronic distribution entrepreneur 2 performs processing which receives and doubles the generated cryptographic key and generates keys A1 and A2 can be considered. In any case of the example of a system, this is considered. Even when taking this employment gestalt, the safety of a system can be secured as compared with the existing distribution model.
[0322] (3-4) the 4- the 6th employment gestalt -- the employment gestalt of these -- the 1- unlike the 3rd employment gestalt, consider the case where the electronic distribution entrepreneur 2 performs encryption processing. That is, it is the case where the electronic distribution entrepreneur 2 receives a cryptographic key from the right person 1 of distribution, and performs cipher processing. In addition, in these examples, the right person 1 side of distribution shall perform coding processing.
[0323] In these cases, it is not because it is [ whether the distribution subject of key information is only the right person 1 of distribution, you are only the electronic distribution entrepreneur 2, or ] the both, but the person in the position in which a cryptographic key can be known despite a join office turns into the contents work firm 1 and two persons of the electronic distribution entrepreneur 2. However, as compared with the existing distribution model, the safety of a system is securable also in this case.
[0324] (3-5) the 7- the 9th employment gestalt -- the employment gestalt of these -- the 4- further in addition to the 6th employment gestalt, consider the case where the electronic distribution entrepreneur 2 also performs activation of coding processing. With these employment gestalten, any longer, because the right person 1 of distribution is generating the cryptographic key, it does not pass over him, but it is not because it is [ whether the distribution subject of key information is only the right person 1 of distribution, you are only the electronic distribution entrepreneur 2, or ] the both, but the person in the position in which a cryptographic key can be known despite a join office turns into the right person 1 of distribution, and two persons of the electronic distribution entrepreneur 2. However, as compared with the existing distribution model, the safety of a system is securable also in this case.
[0325] (3-6) the 10- the 12th employment gestalt -- with the employment gestalt of these, the electronic distribution entrepreneur 2 generates a cryptographic key, and encryption of digital data considers the case where the right person 1 of distribution who received the notice of a cryptographic key from the electronic distribution entrepreneur 2 carries out. The person in the position in which a cryptographic key can be known despite a join office turns into the right person 1 of distribution, and two persons of the electronic distribution entrepreneur 2 irrespective of who becomes the distribution subject of key information also in this case. However, as compared with the existing distribution model, the safety of a system is securable

also in this case.
[0326] (3-7) the 13- the 18th employment gestalt -- the inside of these -- the 13- the 15th employment gestalt is the case where the electronic distribution entrepreneur 2 carries out generation and encryption processing of a cryptographic key, and the right person of distribution performs only coding processing. moreover, the 16- the 18th employment gestalt is the case where the electronic distribution entrepreneur 2 performs both generation of a cryptographic key coding processing and encryption processing.
[0327] Those who are in the position in which a cryptographic key can be known despite a join office irrespective of who becomes the distribution subject of key information in any case of an employment gestalt turn into the right person 1 of distribution, and two persons of the electronic distribution entrepreneur 2. In addition, as compared with the existing distribution model, the safety of a system is securable also in this case.
[0328]
[Effect of the Invention] (1) According to invention according to claim 1 to 5, generate two or more key information on a proper to each distribution person, and the key information on these plurality so that it may be a distribution path different from digital data and may become another distribution path also in both key information That is, by distributing according to an individual using two or more distribution paths, that all information required to restore a cryptographic key comes to hand at once can realize the difficult distribution approach. Moreover, an unjust duplicate can realize the difficult distribution approach also on the transmission line which connects an output unit to a decode server by constituting from a decode server which performs and outputs scramble processing to the digital data of which cipher processing was canceled in the downstream system, and an output unit of which the scramble processing concerned is canceled.
[0329] (2) According to invention according to claim 6, an unjust duplicate can realize a difficult downstream system also on the transmission line which connects an output unit to a decode server by constituting from a decode server which performs and outputs scramble processing to the digital data of which cipher processing was canceled in the downstream system, and an output unit of which the scramble processing concerned is canceled.
[0330] (3) According to invention according to claim 7, from the output signal, the unjust duplicate of digital data can realize a difficult decode server. Moreover, according to invention according to claim 8, the same function as the decode server of claim 7 is realizable only by carrying the circuit apparatus concerned in electronic equipment. Moreover, according to invention according to claim 9, even if it does not use a dedicated device, the same function as the decode server of claim 7 is realizable. Moreover, according to invention according to claim 10, a realizable decode server is [ the same function as the decode server of claim 7 ] easily realizable by

combining with a scramble control section separately. Similarly, according to invention according to claim 11, the same function as the decode server of claim 7 is realizable only by carrying in electronic equipment, combining a circuit apparatus and a scramble control section concerned separately. Moreover, according to invention according to claim 12, by combining with the program as which a computer is operated as a scramble control section, even if it does not use a dedicated device, the same function as the decode server of claim 7 is realizable. Moreover, according to invention according to claim 13, a realizable decode server is [ the same function as the decode server of claim 7 ] easily realizable by combining with invention according to claim 10. Similarly, according to invention according to claim 14, the same function as the decode server of claim 7 is realizable only by carrying in electronic equipment, combining separately a circuit apparatus and a circuit apparatus according to claim 11 concerned. Moreover, according to invention according to claim 15, by combining with a program according to claim 12, even if it does not use a dedicated device, the same function as the decode server of claim 7 is realizable.

[0331] (4) According to invention according to claim 16, from the input signal, the unjust duplicate of digital data can realize a difficult output unit. Moreover, according to invention according to claim 17, the same function as the output unit of claim 16 is realizable only by carrying the circuit apparatus concerned in electronic equipment. Moreover, according to invention according to claim 18, even if it does not use a dedicated device, the same function as the output unit of claim 16 is realizable.

[0332] (5) An unjust duplicate can realize the signal-processing approach in a difficult downstream system also on the transmission line of a decode server and an output unit by according to invention according to claim 19, adopting the structure by which a decode server performs and outputs scramble processing to the digital data of which cipher processing was canceled, and adopting the structure which cancels the scramble processing to which another side and an output unit are given to the digital data, and is outputted with a predetermined output gestalt.

[0333] (6) According to invention according to claim 20, from the output signal, the unjust duplicate of digital data can realize the signal-processing approach in a difficult decode server by adopting the structure by which a decode server performs and outputs scramble processing to the digital data of which cipher processing was canceled.

---

## DESCRIPTION OF DRAWINGS

---

[Brief Description of the Drawings]

[Drawing 1] It is a conceptual block diagram explaining the concept of the distribution

system concerning this invention.
[Drawing 2] It is drawing showing the DS of the data distributed in the network for high-speed distribution in the distribution system concerning this invention.
[Drawing 3] It is drawing showing the case where the distribution system concerning this invention is applied to movie contents.
[Drawing 4] It is the block diagram showing the 1st example of the distribution structure of a system in the gestalt of operation of this invention.
[Drawing 5] It is the block diagram showing the 2nd example of the distribution structure of a system in the gestalt of operation of this invention.
[Drawing 6] It is the block diagram showing the 3rd example of the distribution structure of a system in the gestalt of operation of this invention.
[Drawing 7] It is the block diagram showing the 4th example of the distribution structure of a system in the gestalt of operation of this invention.
[Drawing 8] It is the block diagram showing the 5th example of the distribution structure of a system in the gestalt of operation of this invention.
[Drawing 9] It is the block diagram showing the 6th example of the distribution structure of a system in the gestalt of operation of this invention.
[Drawing 10] It is the block diagram showing the 7th example of the distribution structure of a system in the gestalt of operation of this invention.
[Drawing 11] It is the block diagram showing the 8th example of the distribution structure of a system in the gestalt of operation of this invention.
[Drawing 12] It is the block diagram showing the 9th example of the distribution structure of a system in the gestalt of operation of this invention.
[Drawing 13] It is the block diagram showing the 10th example of the distribution structure of a system in the gestalt of operation of this invention.
[Drawing 14] It is the block diagram showing the 11th example of the distribution structure of a system in the gestalt of operation of this invention.
[Drawing 15] It is the block diagram showing the 12th example of the distribution structure of a system in the gestalt of operation of this invention.
[Drawing 16] It is the block diagram showing the 13th example of the distribution structure of a system in the gestalt of operation of this invention.
[Drawing 17] It is the block diagram showing the 14th example of the distribution structure of a system in the gestalt of operation of this invention.
[Drawing 18] It is drawing which displayed the employment gestalt common to each distribution system shown as an example of a configuration of the gestalt of operation of this invention.
[Description of Notations]
1 Contents Server, 12 Contents Coding Section, 13 Encryption Section, 14 sending-out server, 15 A contents management server, 16 Key generating section, 17 18 A distribution place management server, 26 The doubling key generation section, 19, 21, 22, 25, 27, 28, 29 The write-in section, 20 The partial key generation section, 23 The

multiplex key generation section, 24 Key encryption processing section, 31 A receiving server, 32, 38, 39, 40, 41, 42, 43 Read station, 33 A decode server, 34 Output unit, 34A The descrambling section, 35 A decode function part, 35A The decryption section, 35B The key restoration section, 35C The contents decryption section, 35D The scramble section, 36 scramble control section, 37 Output log Management Department

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－261747
（P2002－261747Ａ）
(43)公開日　平成14年９月13日(2002.9.13)

| (51)Int.Cl.⁷ | 識別記号 | Ｆ１ | | ﾃｰﾏｺｰﾄﾞ(参考) |
|---|---|---|---|---|
| Ｈ０４Ｌ　9/08 | | Ｇ０６Ｆ　15/00 | ３３０Ｚ | ５Ｂ０８５ |
| Ｇ０６Ｆ　15/00 | ３３０ | Ｈ０４Ｌ　9/00 | ６０１Ｂ | ５Ｊ１０４ |

審査請求　有　　請求項の数20　ＯＬ　（全 49 頁）

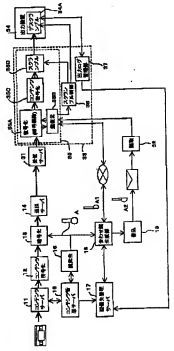
(21)出願番号　特願2001－76918(P2001－76918)
(22)出願日　平成13年３月16日(2001.3.16)
(31)優先権主張番号　特願2000－403472(P2000－403472)
(32)優先日　平成12年12月28日(2000.12.28)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　神谷　成樹
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　山下　雅美
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100067736
弁理士　小池　晃　（外２名）

Ｆターム(参考)　5B085 AE13 AE29 BG07 CA04
5J104 AA01 AA16 AA41 BA03 EA04
EA21 NA02

(54)【発明の名称】　配信方法及び配信システム

(57)【要約】
【課題】　不正行為の困難性とランニングコストの低減要求を両立する。
【解決手段】　復号サーバにおいて暗号処理の解除が許可されるとき、復号サーバ内で発生されたスクランブル鍵を用いて、暗号処理の解除されたディジタルデータをスクランブル処理する。このようにスクランブル処理の施されたディジタルデータを出力装置に与えることで、復号サーバと出力装置とを分離しても、当該伝送経路上で不正行為を行えないようにする。



【特許請求の範囲】

【請求項１】　特定者に対し暗号処理の施されたディジタルデータを多地点配信する上流側システムと、配信を受けたディジタルデータに施されている暗号処理を解除する下流側システムとの間で実行されるディジタルデータの配信方法であって、

上流側システムがその制御下において、

ディジタルデータを対応する暗号鍵で暗号化する処理と、上記暗号鍵を基に配信先である各特定者に固有の複数の鍵情報を生成する処理と、生成された複数の鍵情報をディジタルデータとは別の配信経路であって、鍵情報相互間においても別の配信経路となるものを用いて配信する処理と、暗号処理の施されたディジタルデータを配信する処理とを実行し、

当該ディジタルデータの配信を受ける下流側システムが、

正規の手続きによってのみ開封可能な復号サーバの制御下において、複数の配信経路を通じて配信を受けた複数の鍵情報を基に対応するディジタルデータの暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な出力装置の制御下において、上記復号サーバから入力されるディジタルデータに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行することを特徴とするディジタルデータの配信方法。

【請求項２】　特定者に対し暗号処理の施されたディジタルデータを多地点配信する上流側システムと、配信を受けたディジタルデータに施されている暗号処理を解除する下流側システムとの間で実行されるディジタルデータの配信方法であって、

上流側システムがその制御下において、

ディジタルデータを対応する暗号鍵で暗号化する処理と、上記暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報をディジタルデータとは別の配信経路であって、相互においても別の配信経路となるものを用いて配信する処理と、暗号処理の施されたディジタルデータを配信する処理とを実行し、

当該ディジタルデータの配信を受ける下流側システムが、

正規の手続きによってのみ開封可能な復号サーバの制御下において、複数の配信経路を通じて配信を受けた一組の合わせ鍵又はその発生情報を基に対応するディジタルデータの暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な出力装置の制御下において、上記復号サーバから入力されるディジタルデータに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行することを特徴とするディジタルデータの配信方法。

【請求項３】　特定者に対し暗号処理の施されたディジタルデータを多地点配信する上流側システムと、配信を受けたディジタルデータに施されている暗号処理を解除する下流側システムとの間で実行されるディジタルデータの配信方法であって、

上流側システムがその制御下において、

ディジタルデータを対応する暗号鍵で暗号化する処理と、上記暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、当該複数の部分鍵又はその発生情報とこれら部分鍵の生成に用いなかった残りの合わせ鍵又はその発生情報をディジタルデータとは別の配信経路であって、相互においても別の配信経路となるものを用いて配信する処理と、暗号処理の施されたディジタルデータを配信する処理とを実行し、

当該ディジタルデータの配信を受ける下流側システムが、

正規の手続きによってのみ開封可能な復号サーバの制御下において、複数の配信経路を通じて配信を受けた複数の部分鍵又はその発生情報と、これらと組をなす合わせ鍵又はその発生情報を基に対応するディジタルデータの暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除す

る処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理の解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力する処理とを実行し、
正規の手続きによってのみ開封可能な出力装置の制御下において、上記復号サーバから入力されるディジタルデータに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行することを特徴とするディジタルデータの配信方法。

【請求項４】　特定者に対し暗号処理の施されたディジタルデータを多地点配信する上流側システムと、配信を受けたディジタルデータに施されている暗号処理を解除する下流側システムとの間で実行されるディジタルデータの配信方法であって、
上流側システムがその制御下において、
ディジタルデータを対応する暗号鍵で暗号化する処理と、配信先である各特定者に固有の及び又はディジタルデータに固有の第２の暗号鍵を発生する処理と、上記第２の暗号鍵によって上記第１の生成された合わせ鍵又はその発生情報を暗号化する処理と、当該暗号化された第１の暗号鍵又はその発生情報と上記第２の暗号鍵又はその発生情報をディジタルデータとは別の配信経路であって、相互においても別の配信経路となるものを用いて配信する処理と、暗号処理の施されたディジタルデータを配信する処理とを実行し、
当該ディジタルデータの配信を受ける下流側システムが、
正規の手続きによってのみ開封可能な復号サーバの制御下において、複数の配信経路を通じて配信を受けた第２の暗号鍵又はその発生情報を基に、配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、第１の暗号鍵を復元する処理と、復元された第１の暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力する処理とを実行し、
正規の手続きによってのみ開封可能な出力装置の制御下において、上記復号サーバから入力されるディジタルデータに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行することを特徴とするディジタルデータの配信方法。

【請求項５】　特定者に対し暗号処理の施されたディジタルデータを多地点配信する上流側システムと、配信を受けたディジタルデータに施されている暗号処理を解除する下流側システムとの間で実行されるディジタルデータの配信方法であって、
上流側システムがその制御下において、
ディジタルデータを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の及び又はディジタルデータに固有の第２の暗号鍵を発生する処理と、上記第２の暗号鍵を基に一組の合わせ鍵を生成する処理と、第２の暗号鍵で暗号化された第１の暗号鍵又はその発生情報と上記第２の暗号鍵から生成された一組の合わせ鍵又はその発生情報をディジタルデータとは別の配信経路であって、相互においても別の配信経路となるものを用いて配信する処理と、暗号処理の施されたディジタルデータを配信する処理とを実行し、
当該ディジタルデータの配信を受ける下流側システムが、
正規の手続きによってのみ開封可能な復号サーバの制御下において、複数の配信経路を通じて配信を受けた一組の合わせ鍵又はその発生情報を基に第２の暗号鍵を復元して、配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、第１の暗号鍵を復元する処理と、復元された第１の暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理において生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力する処理とを実行し、
正規の手続きによってのみ開封可能な出力装置の制御下において、上記復号サーバから入力されるディジタルデータに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行することを

特徴とするディジタルデータの配信方法。

【請求項６】　暗号処理の施されたディジタルデータの配信を受けて所定の信号処理を実行する復号サーバと、所定の出力形態でコンテンツを出力する出力装置とを備える電子配信システムにおける下流側システムであって、

上記復号サーバは、配信段階でディジタルデータに施された暗号処理を解除する暗号解除部と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成するスクランブル制御部と、上記暗号解除部で暗号処理が解除されたディジタルデータの唯一の出力先であって、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する復号化部と、復元されたディジタルデータの唯一の出力先であって、上記スクランブル制御部において生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力するスクランブル処理部とを備え、

上記出力装置は、上記受信サーバから入力されるディジタルデータに施されているスクランブル処理を、上記受信サーバから与えられたスクランブル解除鍵によって解除するスクランブル解除部と、上記スクランブル解除部でスクランブルが解除されたディジタルデータの唯一の出力先であって、当該ディジタルデータを所定の出力形態で出力する信号処理部とを備えることを特徴とする電子配信システムにおける下流側システム。

【請求項７】　暗号処理の施されたディジタルデータの配信を受け所定の信号処理を実行する電子配信システムにおける復号サーバであって、

配信段階でディジタルデータに施された暗号処理を解除する暗号解除部と、

ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成するスクランブル制御部と、

上記暗号解除部で暗号処理が解除されたディジタルデータの唯一の出力先であって、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する復号化部と、

復元されたディジタルデータの唯一の出力先であって、上記スクランブル制御部において生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力するスクランブル処理部とを備えることを特徴とする電子配信システムにおける復号サーバ。

【請求項８】　暗号処理の施されたディジタルデータの配信を受けて所定の信号処理を実行する電子配信システムにおける復号サーバの機能を実現する回路装置であって、

配信段階でディジタルデータに施された暗号処理を解除する暗号解除部と、

ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成するスクランブル制御部と、

上記暗号解除部で暗号処理が解除されたディジタルデータの唯一の出力先であって、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する復号化部と、

復元されたディジタルデータの唯一の出力先であって、上記スクランブル制御部において生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力するスクランブル処理部とを備えることを特徴とする回路装置。

【請求項９】　コンピュータに、配信段階でディジタルコンテンツに施された暗号処理を解除する暗号解除処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成するスクランブル制御処理と、上記暗号解除処理で暗号処理が解除されたディジタルデータの唯一の出力先として、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する復号化処理と、復元されたディジタルデータの唯一の出力先として、上記スクランブル制御処理において生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力するスクランブル処理を実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項１０】　暗号処理の施されたディジタルデータの配信を受け所定の信号処理を実行する電子配信システムにおける復号サーバであって、

配信段階でディジタルデータに施された暗号処理を解除する暗号解除部と、

上記暗号解除部で暗号処理が解除されたディジタルデータの唯一の出力先であって、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する復号化部と、

復元されたディジタルデータの唯一の出力先であって、スクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力するスクランブル処理部とを備えることを特徴とする電子配信システムにおける復号サーバ。

【請求項１１】　暗号処理の施されたディジタルデータの配信を受けて所定の信号処理を実行する電子配信システムにおける復号サーバの機能を実現する回路装置であって、

配信段階でディジタルデータに施された暗号処理を解除する暗号解除部と、

上記暗号解除部で暗号処理が解除されたディジタルデータの唯一の出力先であって、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する復号化部と、

復元されたディジタルデータの唯一の出力先であって、

所定のスクランブル鍵を用いディジタルデータの元データをスクランブル処理して出力するスクランブル処理部とを備えることを特徴とする回路装置。

【請求項１２】　コンピュータに、配信段階でディジタルデータに施された暗号処理を解除する暗号解除処理と、上記暗号解除処理で暗号処理が解除されたディジタルデータの唯一の出力先として、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する復号化処理と、復元されたディジタルデータの唯一の出力先として、所定のスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力するスクランブル処理を実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項１３】　配信を受けたディジタルデータに施されている暗号処理を解除する復号サーバであって、
ディジタルデータに付属する再生条件が満たされることを条件に、出力装置に出力されるディジタルデータの局所暗号化用のスクランブル鍵と当該スクランブル鍵で暗号化されたディジタルデータの出力装置側での局所復号化用の解除鍵を生成するスクランブル制御部を備えることを特徴とする復号サーバ。

【請求項１４】　配信を受けたディジタルデータに施されている暗号処理を解除する復号サーバの機能を実現する回路装置であって、
ディジタルデータに付属する再生条件が満たされることを条件に、復号サーバから出力装置に出力されるディジタルデータの局所暗号化用のスクランブル鍵と当該スクランブル鍵で暗号化されたディジタルデータの出力装置側での局所復号化用の解除鍵を生成するスクランブル制御部を備えることを特徴とする回路装置。

【請求項１５】　コンピュータに、配信を受けたディジタルデータに付属する再生条件が満たされることを条件に、復号サーバから出力装置に出力されるディジタルデータの局所暗号化用のスクランブル鍵と当該スクランブル鍵で暗号化されたディジタルデータの出力装置側での局所復号化用の解除鍵を生成するスクランブル制御処理を実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項１６】　コンテンツを所定の出力形態で出力する電子配信システム対応の出力装置であって、
復号サーバから入力されるディジタルデータに施されているスクランブル処理を、上記復号サーバ側から与えられたスクランブル解除鍵によって解除するスクランブル解除部と、
上記スクランブル解除部でスクランブルが解除されたディジタルデータの唯一の出力先であって、当該ディジタルデータを所定の出力形態で出力する信号処理部とを備えることを特徴とする電子配信システム対応の出力装置。

【請求項１７】　コンテンツを所定の出力形態で出力する電子配信システム対応の出力装置に搭載可能な回路装置であって、
上記復号サーバから入力されるディジタルデータに施されているスクランブル処理を、上記復号サーバ側から与えられたスクランブル解除鍵によって解除するスクランブル解除部を備えることを特徴とする回路装置。

【請求項１８】　復号サーバから入力されるディジタルデータに施されているスクランブル処理を、所定のスクランブル解除鍵によって解除するスクランブル解除処理を、コンピュータに実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項１９】　特定者のみが再生できるように暗号処理の施されたディジタルデータの配信を受けて所定の信号処理を実行する復号サーバと、所定の出力形態でコンテンツを出力する出力装置とを備える電子配信システムにおける下流側システムの信号処理方法であって、
正規の手続きによってのみ開封可能な上記復号サーバが、配信段階でディジタルデータに施された暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、上記処理で暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力する処理とを実行し、
正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるディジタルデータに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行することを特徴とする電子配信システムにおける下流側システムの信号処理方法。

【請求項２０】　暗号処理の施されたディジタルデータの配信を受けて所定の信号処理を実行する電子配信システムにおける復号サーバの信号処理方法であって、
正規の手続きによってのみ開封可能な上記復号サーバが、配信段階でディジタルデータに施された暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生

成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力する処理とを実行することを特徴とする電子配信システムにおける復号サーバの信号処理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はディジタルデータの配信方法及び配信システムに関する。また、本発明は、ディジタルデータの配信方法及び配信システムの実現に必要な要素技術に関する。

【０００２】

【従来の技術】ディジタル技術の進展に伴い、あらゆるディジタルデータ（文字データ（例えば、テキスト、記号、図形）、オーディオデータ（例えば、音声、楽曲）、ビデオデータ（例えば、静止画、動画）、オーディオデータとビデオデータの複合データ（例えば、映画、放送番組）、プログラムデータ、データベースデータその他のディジタルデータ）がネットワークや記録媒体を通じて配信されようとしている。

【０００３】なお配信されるディジタルデータは、単一のデータファイルからなる場合もあれば、複数のデータファイルから構成される場合もある。またデータファイルに関しても、単一のコンテンツの情報のみを含むものもあれば、複数のコンテンツの情報が含まれるものもある。またコンテンツは複数のディジタルデータに分散される場合もある。

【０００４】

【発明が解決しようとする課題】一方、ディジタルデータは完全な複製物を容易に作成できるため、不正行為（例えば、不正復号再生、不正複製、横流し）が行われると、非常に大きな損害が生じてしまう。このため、不正行為からコンテンツ提供者（例えば、コンテンツ制作者、配給権者、配信事業者）を保護する仕組み作りが急がれている。特に、制作に膨大な費用と人手を要し、資産価値の高いコンテンツ（例えば、映画）に関しては、不正行為によって莫大な損害が生じるため、不正行為が困難な仕組み作りが求められる。

【０００５】しかし、防御能力が高いものは多大な設備投資を必要としたり、設備投資が比較的少なくて済むものは防御能力に問題がある等、コンテンツ提供者と受け手の双方が納得できるような仕組みは確立されていないのが現状である。

【０００６】例えば、不正行為に対する耐性を高く保ち続けたり、より再現性の高い出力技術が現れた場合には適宜最新の技術を導入できることが望ましいが、現在提案されているビジネスモデルでは受け手側に必要な機能を全て出力装置内に設ける構成を採るため、技術寿命の短いものに合わせて出力装置自体の買い替えが必要となる。しかし、出力装置の短期間での買い替えを前提とするビジネスモデルでは、受け手側の理解を得ることができない。またその結果として、陳腐化した技術の置き換えが進み難く、ディジタルデータが不正行為にあう危険性が高まるという弊害がある。

【０００７】このため、資産価値の高いコンテンツの提供がコンテンツ制作者に認められなかったり、ビジネスモデル自体が受け手側に受け入れられず、システムの運用を開始できない等の問題が生じている。

【０００８】本願明細書は以上の課題を考慮し、ディジタルデータの配信段階から最終出力段階に至るまで不正行為が極めて難しく、しかも合理的な対価によって長期にわたって高い防御機能を維持できる配信方法及び当該方法を適用したシステム並びにそれらを実現する要素技術について提案する。

【０００９】

【課題を解決するための手段】かかる課題を解決するため以下の手段を提案する。

【００１０】（１）本願明細書で想定する配信モデル

以下の各手段では後述する処理を実行する上流側システムと下流側システムとで構成される配信モデルを想定する。

【００１１】まず上流側システムとして、暗号処理の施されたディジタルデータを多地点配信するものを想定する。ここでの暗号化処理は、配信対象であるディジタルデータ毎に固有なもの（すなわち配信対象であるディジタルデータ毎に固有の暗号鍵で暗号化する）でも良いが、必ずしもこれに限らない。勿論、配信対象であるディジタルデータ毎に固有のものを使用すれば、不正行為が行われてもその被害が当該ディジタルデータ単位でしか生じないため、被害を最小化できる利点がある。ただし、システムの信頼性が高い場合や簡易な配信システムが望まれる場合には、複数のディジタルデータについて共通の暗号処理を採用する場合もあり得る。いずれの暗号化処理を採用するかは、ビジネス上の要請による。またここでの多地点配信には、放送による配信や通信による配信のように伝送媒体を通じて行う態様の配信の他、記録媒体を用いて物理的に行う配信も含まれる。

【００１２】また、上流側システムは、ディジタルデータの暗号化に使用した暗号鍵の配信に際し、例えば以下に示すような方法のいずれかによって配信先やディジタルデータに固有の複数の鍵情報を作成し、それらをディジタルデータとは別の配信経路（媒体を物理的に異にするもの、又は、配信時間帯を異にするもの。以下同じ。）であって、鍵情報相互間においても別の配信経路となるものを通じて対応する配信先、すなわち下流側システムに配信する方式を採用する。すなわち、鍵情報を複数の経路を通じて配信することにより、いずれかの経路を通じて配信される鍵情報が盗まれた場合でも、他の全ての鍵情報が盗まれない限り被害の発生を防止できるようにする。なお配信される鍵情報は、暗号鍵そのものだけでなく、その発生情報（例えば、乱数）でもよい。

また鍵情報は、暗号鍵を分割した合わせ鍵や部分鍵でもよい。因みに暗号化方式は共通鍵方式でも公開鍵方式でも良い。またこれらの複合方式でも良い。

【００１３】上述の方法としては、例えば

１）暗号鍵を配信先毎に固有の分割パターンで分割し、一組（一対のみならず、３個以上の場合も含まれる。）の部分鍵を生成する方法

２）配信先毎に固有の異なる暗号鍵（請求項における第２の暗号鍵）を生成すると共に、当該暗号鍵でディジタルデータの暗号化に使用した暗号鍵（請求項における第１の暗号鍵）を暗号化したものを生成する方法

３）ディジタルデータ毎に固有の異なる暗号鍵（請求項における第２の暗号鍵）を生成すると共に、当該暗号鍵でディジタルデータの暗号化に使用した暗号鍵（請求項における第１の暗号鍵）を暗号化したものを生成する方法がある。

【００１４】なお配信先毎に固有の異なる暗号鍵（請求項における第２の暗号鍵）は、１つに限る必要はなく２つ以上使用しても良い。この場合、複数の第２の暗号鍵で第１の暗号鍵を２回以上（多重）暗号化すれば良い。いずれにしても、第１の暗号鍵が第２の暗号鍵で１回以上暗号化される点で違いはない。また第２の暗号鍵とは別の暗号鍵（例えば、配信先の違いによらず共通に使用する暗号鍵、ディジタルデータ毎に固有の暗号鍵、複数のディジタルデータに共通の暗号鍵、その他の暗号鍵）を組み合わせることで暗号処理を多重的に実行する等さまざまな暗号化手法が考えられる。

【００１５】ここでの配信先毎に固有の分割パターンや配信先毎に固有の異なる暗号鍵は、配信者毎にほぼ普遍的に割り当てられている場合もあれば（ディジタルデータの違いによらず、比較的長期に同じ暗号鍵を使用する場合もあれば）、配信対象であるディジタルデータ毎にその都度割り当てられる場合もある。勿論、不正行為対策の観点からは後者が望ましい。

【００１６】なお多地点配信の手法には、伝送網（ネットワーク）を用いて電子的に配信する方法の他、記録媒体を用いて物理的に配信する方法も含まれる。

【００１７】次に、下流側システムとして、配信されたディジタルデータを復号する復号サーバと、復号されたコンテンツを所定の形態で出力する出力装置とが物理的に分離されているものを想定する。すなわち、復号サーバは、ディジタルデータとは別の複数の配信経路を通じて配信を受けた複数の鍵情報から元の暗号鍵を復元し、ディジタルデータに施されている暗号処理を解除する処理と、所定の信号処理の施されたディジタルデータを出力装置への出力用にスクランブル処理する処理とを実行するものを考える。

【００１８】このように暗号処理の復号機能を出力装置とは別に設けるようにしたことにより、受け手側にとって設備の更新負担が少なくて済むシステム構成とできる。すなわち、配信システムの運用開始後に暗号方式の変更を行う場合にも、復号サーバだけを更新すればよく、暗号処理の復号とは関係のない出力装置については性能に支障のない限りそのまま使用できるようになる。同様に、出力装置をより性能の高いものに置き換える場合でも何らの問題のない復号サーバについてはそのまま使用できるようになる。かかる仕組みは長期的な運用コストを低減する上で効果的である。

【００１９】もっとも、復号機能と出力装置を単に分離しただけでは不正行為に対して極めて無防備な配信モデルとなってしまうが、復号サーバと出力装置との間を流れるデータをスクランブル処理されたディジタルデータとすることにより、復号サーバと出力装置との間を流れるディジタルデータを不正に入手してもコンテンツ自体を入手できないようになっている。

【００２０】なお、復号サーバや出力装置においても不正行為の起こり得ない仕組みを採用する。例えば、正規の手続き以外では復号サーバや出力サーバの筐体を開封できない仕組みや不正に開封すると動作しなくなる仕組みを採用する。また、復号サーバにおいて実行される特定の処理機能を集積回路化して処理の過程で現れる暗号鍵や生のディジタルデータが取り出されないようにする仕組みを採用する。ここで正規の手続きとしては、例えば開封する資格を有する者のみが保持する電子的な鍵や物理的な鍵を使用することが考えられる。また、不正に開封する行為としては、例えば筐体を破壊することが考えられる。

【００２１】（２）配信モデルを実現する代表的な手段以下、配信モデルを実現する代表的な手段について説明する。ここでの配信モデルは、前述のように上流側システムと下流側システムとで構成される配信システムを前提とする。また以下では、配信モデル全体からみた配信方法について説明する。なお上流側システムと下流側システムとは別の事業者によって構築される場合が一般的と予想されるが、ディジタルデータに施されている暗号処理を解除する処理までの処理までを上流側システムの事業者が受け持つような運用形態を排除するものではない。

【００２２】上流側システムの運営形態には様々な形態が考えられる。例えば、単一の事業者が上流側システムを運営する形態や複数の事業者が共同して上流側システムを運営する場合が考えられる。このため、以下の各手段を構成する各処理は、単一の事業者によって行われる場合だけでなく、複数の事業者によって行われる場合もあり得る。

【００２３】ここで単一の事業者としては、例えば、ディジタルデータの配給権を有すると共に、ディジタルデータの配信事業も行うものを想定する。なお単一の事業者には実質的に単一とみなすことができるものも含み得る。例えば、ある会社の税法上の子会社ではないが一定

の資本関係の認められる関連会社や子会社が処理を分担して実施する場合も考えられる。もっともこれらは、後述するように、複数の事業者による実施とも考えられる。

【００２４】上流側システムが複数の事業者によって実施される場合、各処理機能がいずれの事業者に振り分けられるかはビジネス上の要請による。従って、各事業者で用いられる具体的なハードウェアの構成やソフトウェアの構成は各処理の組み合わせに応じて種々のものが考えられる。

【００２５】例えば、ディジタルデータを暗号化するまでの処理と各配信先に応じた複数の鍵情報を生成する処理については配給権を有する事業者が実行し、配信事業者は暗号化されたディジタルデータの配信のみを行うようにすると、暗号鍵（マスター鍵）を知り得るのは配給権を有する事業者のみとできる。このため、かかる運営形態を採用する場合には、配給権を有する事業者にとって安全性を保持し易いシステムとできる。ここで配給権を有する事業者としては、例えばディジタルデータの制作者から配給権を得た事業者（コンテンツ制作者とは別の事業者である場合もあれば、コンテンツ制作者と同一の事業者である場合も含む。）が考えられる。

【００２６】なお以下の各手段では、電子透かしについて言及していないが、不正行為の防止や流出経路の特定の観点からはディジタルデータを暗号化する前に、固有の電子透かしを入れておくことが望ましい。現実にはほとんどの場合に電子透かしが入れられると考えられる。

【００２７】また、暗号化されたディジタルデータの配信に際し、配信事業者や伝送網の管理者が別途他の暗号処理を施すことは自由である。また、鍵情報を配信する場合にも実際は、電子証明書（信頼できる第３者機関である認証局がディジタル署名したもの）等によって相手先が真正な配信先であることを確認し、その上で相手方の公開鍵で鍵情報を暗号化しておくことが安全を期する上で望ましい。

【００２８】なお以下の手段では、分割処理によって暗号鍵から直接得られる鍵を「合わせ鍵」と、合わせ鍵を更に分割することで得られる鍵を「部分鍵」というものとする。もっとも、いずれの鍵も暗号鍵の一部分である点では同じである。また以下の手段では、暗号鍵を暗号化するのに使用する鍵を「多重鍵」というものとする。なお、暗号鍵の暗号化処理は１回のみならず２回、３回というように多数回重畳的に行う場合も当然含まれる。

【００２９】また各手段において鍵情報を配信する場合には、鍵情報の伝送網にディジタルデータの伝送網と物理的に同じものを用いることも可能である。ただし、その場合にはディジタルデータと鍵情報とを同時刻に配信することはせず、それぞれの配信時間帯をずらし、実際上、別経路で配信するのと同様の状態で配信を行うことが望ましい。これは、ディジタルデータとその鍵情報とを同一の配信経路を通じて同時配信すると、１回の不正行為でディジタルデータと鍵情報の一部を同時に入手できるため、その分、ディジタルデータに施されている暗号が解除される危険性が高まるためである。

【００３０】なお各手段のいずれの場合にも、下流側システムは配信を受ける鍵情報から暗号鍵を復元するのに必要な情報を予め知っているか、上流側システムから通知されるものとする。勿論、上流側システムから当該情報が通知されるタイミングは鍵情報の配信と同時でも良いし、別のタイミングでも良い。

【００３１】（２－１）第１の手段

第１の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。なお、上流側システムは前述のように、ディジタルデータの配給権を有する事業者単独で運営される場合もあれば、当該配給権を有する事業者とディジタルデータの配信を実行する配信事業者とで運営される場合もある。また、下流側システムは前述のように、ディジタルデータに施されている暗号処理を解除する復号サーバと、ディジタルデータを所定の出力形態で出力する出力装置とで構成されるものである。これらは後述する他の手段においても同様である。

【００３２】上流側システムがその制御下において、ディジタルデータを対応する暗号鍵で暗号化する処理と、上記暗号鍵を基に配信先である各特定者に固有の一組（一対のみならず、３個以上の組み合わせも含む。他の手段について同じ。）の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報をディジタルデータとは別の配信経路であって、相互においても別の配信経路となるものを用いて配信する処理と、暗号処理の施されたディジタルデータを配信する処理とを実行するものを提案する。

【００３３】また下流側システム（個々の配信先毎に設けられる。）では、正規の手続きによってのみ開封可能な復号サーバの制御下において、複数の配信経路を通じて配信を受けた一組の合わせ鍵又はその発生情報を基に対応するディジタルデータの暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力する処理とを実行するものを提案する。

【００３４】また正規の手続きによってのみ開封可能な出力装置の制御下において、上記復号サーバから入力さ

れるディジタルデータに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行するものを提案する。

【００３５】第１の手段は要するに、ディジタルデータの暗号化に使用した暗号鍵を、各配信先（下流側システム）に固有の分割規則で分割して一組（例えば３個）の合わせ鍵を生成し、それらをディジタルデータとは別の配信経路であって、合わせ鍵相互においても別の配信経路となるものを用いて配信する方式と、配信を受けた鍵情報から復元された暗号鍵を用い暗号処理の解除されたディジタルデータにスクランブル処理を施したものを出力装置に出力する再生方式とを組み合わせたものである。

【００３６】この第１の手段では信号処理の観点から説明しているが、これらの処理機能を備えるハードウェア構成によって実現することも可能であるし、周様の機能をソフトウェア処理として実現することも可能である。後述する他の手段についても同様である。この場合、ハードウェアやソフトウェア（コンピュータに該当処理を実行させるプログラムを記録した記録媒体、プログラム自体その他のプログラムプロダクト）は上流側システムと下流側システムのそれぞれについて用意する。なおハードウェアには、復号サーバや出力装置といった完成品の他、インターフェースボードや半導体集積回路等といった構成部品（請求項における回路装置）が考えられる。

【００３７】かかる第１の手段を用いることにより、複数の配信経路を通じて配信される複数の鍵情報のうちいずれかが盗難されたとしても残る全ての鍵情報も盗難されない限り暗号鍵の流出を防止できる配信モデルを提供できる。特に、鍵情報をディジタルデータとは別の経路（上述のように同一の媒体を用いながら時間的に別の時間帯に配信する場合を含む。）で配信する場合には、鍵情報の一部を盗んだ不正行為者が暗号化されたディジタルデータをも入手した場合でも、暗号鍵の復元に必要な鍵情報はディジタルデータとは別に配信されるため、生のディジタルデータが復号化される事態をより困難にできる。

【００３８】またこの第１の手段では、復号処理されたディジタルデータを局所的にスクランブル処理したものを出力装置に出力する方式を採用したことにより、復号サーバと出力装置を物理的に別の装置とする場合でも当該装置間において生のディジタルデータが流出するおそれを確実に回避できる配信モデルを提供できる。しかもその結果として、復号サーバや出力装置の開発負担を軽減できる。かくして、復号サーバや出力装置の価格の低下を実現でき、配信サービスの利用者にとっても導入し易いシステムとできる。また、長期の運用を考慮した場合にも最新の技術への置き換えが低い費用で進み易く、サービスの提供側にも利用者側にも好ましい仕組みを実現できる。かかる効果は他の手段についても同様である。

【００３９】なお第１の手段では、ディジタルデータの暗号化に対応する暗号鍵が既に存在することを前提にするが、当該暗号鍵は上流側システム内で発生しても良いし、上流側システムの外部より与えられるものでも良い。ここでの暗号鍵は各ディジタルデータに固有のものでも良いし、複数のディジタルデータに共通のものでも良い。前者の鍵を使用する場合には、暗号鍵がたとえ最終的に解読されたとしてもその被害を当該ディジタルデータに限定することができる。もっとも、後者の鍵を使用する場合でも、比較的頻繁に鍵を変更することにより盗難時の被害が及ぶ範囲を限定できる。なお、このディジタルデータの暗号化に使用する暗号鍵についての説明は他の手段についても同様である。

【００４０】因みに第１の手段における鍵情報の配信方法としては、例えば次のようなものを採り得る。例えば、一組の合わせ鍵の一部を伝送網（ネットワーク）を通じて配信し、その他を記録媒体を通じて配信する方法を採り得る。このように鍵情報の一部を有体物である記録媒体の形態で配信すると、鍵情報の盗難を発見し易く、不正行為に対する対抗策をいち早く実施できる。

【００４１】また例えば、一組の合わせ鍵の一部を第１の伝送網（ネットワーク）を通じて配信し、その他を第２の伝送網（ネットワーク）を通じて配信する方法を採り得る。このように全ての鍵情報を伝送網を通じて配信すると、鍵情報の配信に要する時間的制約を少なくできる。また鍵情報の配信を経済的に実施できる。なお以上の伝送網（ネットワーク）を用いた鍵情報の配信に際しては、例えば電子証明書を使用して本人確認（配信先の確認）を行い、認証された配信先が公開する公開鍵で暗号化した鍵情報を配信するなどの手法が望ましい。

【００４２】また例えば、一組の合わせ鍵の一部を第１の記録媒体を介して配信し、その他を第２の記録媒体を介して配信する方法を採り得る。このように全ての鍵情報を有体物である記録媒体の形態で配信すると、鍵情報の盗難をより一層発見し易くでき、不正行為に対する対抗策をいち早く実施できる。勿論、２つの記録媒体には物理的に異なる媒体を使用する。言うまでもなく、記録媒体の種類や読み取り方式については同じでも、異なっても構わない。

【００４３】ここで、合わせ鍵の配信に使用する記録媒体には、磁気読み取り方式の媒体（例えば、磁気テープ、フロッピー（登録商標）ディスク、磁気カード）、光学読み取り方式の媒体（例えば、ＣＤ－ＲＯＭ、ＭＯ、ＣＤ－Ｒ、ＤＶＤ）、半導体メモリ（メモリカード（矩形型、正方形型など形状は問わない。）、ＩＣカー

ド）その他が考えられる。当該記録媒体の配信には、郵便制度や宅配制度を使用する。現行の制度では、秘匿性の観点から書留郵便が選択される場合が多いと考えられる。この配信用の記録媒体についての記載は以下の各手段についても共通である。また、ディジタルデータの配信に用いる場合の記録媒体についても同様である。

【００４４】また、前述の出力装置としては表示装置（例えば、モニタ装置、テレビジョン受像機、プロジェクタ装置、携帯型の電子機器）、印刷装置、スピーカ、記録媒体への記録装置等が考えられる。ここで、出力装置における所定の出力形態には、ディジタルデータが例えばビデオデータであれば、表示画面への表示、投影面への投影が考えられる。またディジタルデータが例えばオーディオデータであれば、スピーカを通じての出力が考えられる。勿論、オーディオデータとビデオデータの複合データであれば、その同時に２つの出力が行われる。

【００４５】（２－２）第２の手段

第２の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【００４６】上流側システムがその制御下において、ディジタルデータを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、当該複数の部分鍵又はその発生情報とこれら部分鍵の生成に用いなかった残りの合わせ鍵又はその発生情報をディジタルデータとは別の配信経路であって、相互においても別の配信経路となるものを用いて配信する処理と、暗号処理の施されたディジタルデータを配信する処理とを実行するものを提案する。

【００４７】また下流側システム（個々の配信先毎に設けられる。）では、正規の手続きによってのみ開封可能な復号サーバの制御下において、複数の配信経路を通じて配信を受けた複数の部分鍵又はその発生情報と、これらと組をなす合わせ鍵又はその発生情報を基に対応するディジタルデータの暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理の解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力する処理とを実行するものを提案する。

【００４８】また正規の手続きによってのみ開封可能な出力装置の制御下において、上記復号サーバから入力されるディジタルデータに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行するものを提案する。

【００４９】第２の手段は要するに、ディジタルデータの暗号化に使用した暗号鍵を、各配信先（下流側システム）に固有の分割規則で分割して一組（例えば３個）の合わせ鍵とし、その一部（例えば２個）はそのまま配信し、その他（この場合１個）は例えば分割して複数の部分鍵を生成しこれを配信する方式と、配信を受けた鍵情報から復元された暗号鍵を用い暗号処理の解除されたディジタルデータにスクランブル処理を施したものを出力装置に出力する再生方式とを組み合わせたものである。勿論、これら鍵情報の配信には、ディジタルデータとは別の配信経路であり、かつ各鍵情報相互間においても別の配信経路となるものを使用する。

【００５０】かかる第２の手段を用いれば、複数の配信経路を通じて配信される複数の鍵情報のうちいずれかが盗難されたとしても残る全ての鍵情報も盗難されない限り暗号鍵の流出を防止できる配信モデルを提供できる。しかもこの第２の手段の場合には、第１の手段よりも更に鍵情報の配信経路を増やせるため、より不正行為に対する安全性の高い配信モデルを提供できる。

【００５１】なお合わせ鍵から一組の部分鍵を生成するのに用いる分割規則は、全ての配信先に共通の規則でも良いし、各配信先に固有の規則でも良いし、特定地域その他の条件で区分された配信先の集合毎に固有の規則でも良い。他の手段においても同様である。

【００５２】なおここでの部分鍵の生成方法には、合わせ鍵の一部を更に分割する方法の他、合わせ鍵の一部を多重鍵する方法もある。後者の場合、暗号化された鍵情報とその暗号化に使用した暗号鍵が配信対象となる。同様の仕組みを採用する他の手段についても同様である。

【００５３】因みに第２の手段における鍵情報の配信方法としては、例えば次のようなものを採り得る。例えば、合わせ鍵の一部を伝送網（ネットワーク）を通じて配信し、その他の合わせ鍵から生成される部分鍵の一部を伝送網（ネットワーク）で配信し、残る部分鍵を記録媒体で配信する方法を採り得る。このように鍵情報の一部を有体物である記録媒体の形態で配信することで鍵情報の盗難を発見し易くでき、不正行為に対する対抗策をいち早く実施できる。なお言うまでもなく、記録媒体による配信はいずれの鍵情報でも良いし、任意の２種類の鍵情報をそれぞれ別の記録媒体で配信することもできる。

【００５４】また例えば、一組の合わせ鍵の一部と、残る合わせ鍵から生成した部分鍵の全てを伝送網（ネット

ワーク）で配信する方法を採り得る。このように全ての鍵情報を伝送網（ネットワーク）を介して配信すると、鍵情報の配信に要する時間的制約を少なくできる。また鍵情報の配信を経済的に実施できる。なお以上の伝送網（ネットワーク）を用いた鍵情報の配信に際しては、例えば電子証明書を使用して本人確認（配信先の確認）を行い、認証された配信先が公開する公開鍵で暗号化した鍵情報を配信するなどの手法が望ましい。

【００５５】また例えば、一組の合わせ鍵の一部と、残る合わせ鍵から生成した部分鍵の全てを記録媒体で配信する方法を採り得る。このように全ての鍵情報を有体物である記録媒体を介して配信すると、鍵情報の盗難をより一層発見し易くでき、不正行為に対する対抗策をいち早く実施できる。勿論、鍵情報の配信に使用する記録媒体はそれぞれ媒体の形態が異なっていても良いし、読み取り方式が異なっていても良い。

【００５６】（２－３）第３の手段

第３の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【００５７】上流側システムがその制御下において、ディジタルデータを対応する暗号鍵で暗号化する処理と、配信先である各特定者に固有の及び又はディジタルデータに固有の第２の暗号鍵を発生する処理と、上記第２の暗号鍵によって上記第１の生成された合わせ鍵又はその発生情報を暗号化する処理と、当該暗号化された第１の暗号鍵又はその発生情報と上記第２の暗号鍵又はその発生情報をディジタルデータとは別の配信経路であって、相互においても別の配信経路となるものを用いて配信する処理と、暗号処理の施されたディジタルデータを配信する処理とを実行するものを提案する。

【００５８】また下流側システム（個々の配信先毎に設けられる。）では、正規の手続きによってのみ開封可能な復号サーバの制御下において、複数の配信経路を通じて配信を受けた第２の暗号鍵又はその発生情報を基に、配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、第１の暗号鍵を復元する処理と、復元された第１の暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力する処理とを実行するものを提案する。

【００５９】また正規の手続きによってのみ開封可能な出力装置の制御下において、上記復号サーバから入力されるディジタルデータに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行するものを提案する。

【００６０】第３の手段は要するに、ディジタルデータの暗号化に使用した暗号鍵（第１の暗号鍵）を第２の暗号鍵で暗号化してなる暗号鍵と、その暗号化に使用した第２の暗号鍵を、ディジタルデータとは別の配信経路を用い、かつ、各暗号鍵相互においても別の配信経路となるものを用いて配信する方式と、配信を受けた鍵情報から復元された暗号鍵を用い暗号処理の解除されたディジタルデータにスクランブル処理を施したものを出力装置に出力する再生方式とを組み合わせたものである。

【００６１】かかる第３の手段を用いることにより、複数の配信経路を通じて配信される複数の鍵情報のうちいずれかが盗難されたとしても残る全ての鍵情報も盗難されない限り暗号鍵の流出を防止できる配信モデルを提供できる。特に、鍵情報をディジタルデータとは別の経路（上述のように同一の媒体を用いながら時間的に別の時間帯に配信する場合を含む。）で配信する場合には、鍵情報の一部を盗んだ不正行為者が暗号化されたディジタルデータをも入手した場合でも、暗号鍵の復元に必要な鍵情報はディジタルデータとは別に配信されるため、生のディジタルデータが復号化される事態をより困難にできる。

【００６２】なお第２の暗号鍵として配信先である各配信者に固有のものを用いる場合には、特定の配信者から全ての鍵情報（第２の暗号鍵と暗号化された第１の暗号鍵）を盗難しない限り、ディジタルデータに施されている暗号を解除できない。すなわち、ある配信者に宛てて配信された固有の第２の暗号鍵と、ある配信者に宛てて配信された暗号化された第１の暗号鍵を盗難したとしても、第１の暗号鍵を取り出すことはできない。勿論、暗号化されたディジタルデータも盗難しなければディジタルデータ自体の盗難はできない。なお、全てのデータを不正行為が発覚する前に盗難することは事実上困難であり、不正行為に強いシステムとできる。

【００６３】また第２の暗号鍵としてディジタルデータに固有のものを用いる場合には、第２の暗号鍵と当該第２の暗号鍵で暗号化された第１の暗号鍵が盗難された場合でも、その被害を特定のディジタルデータ（勿論、暗号化されたディジタルデータも盗難されることが前提となる。）に限定できる。言うまでもなく、この場合も全てのデータを不正行為の発覚前に盗難することは事実上困難であり、不正行為に強いシステムとできる。

【００６４】なお言うまでもないが、第２の暗号鍵として配信先である各配信者について固有であり、かつディジタルデータについても固有のものを用いれば、より盗

難の難しいシステムとできる。上述のいずれの暗号鍵を採用するかは、配信対象であるディジタルデータの経済的価値やディジタルデータの運用ポリシーによる。

【００６５】因みに第１の暗号鍵の暗号化は第２の暗号鍵で少なくとも１回行えば良く、他の種類の暗号鍵で暗号化する処理と組み合わせても良い。従って、第２の暗号鍵で暗号化する前に既に第１の暗号鍵が暗号化されていても良い。このような場合でも第１の暗号鍵が第２の暗号鍵で暗号化されていることに技術上の違いはない。

【００６６】なお第３の手段における鍵情報の配信方法としては、例えば次のようなものを採り得る。例えば、暗号化された第１の暗号鍵を伝送網（ネットワーク）を通じて配信し、第２の暗号鍵を記録媒体を通じて配信する方法を採り得る。このように鍵情報の一部を記録媒体の形態で配信すると、鍵情報の盗難を発見し易く、不正行為に対する対抗策をいち早く実施できる。なお上述の場合とは反対に、暗号化された第１の暗号鍵を記録媒体を通じて配信し、第２の暗号鍵を伝送網（ネットワーク）を通じて配信する方法を採ることもできる。

【００６７】また例えば、暗号化された第１の暗号鍵を第１の伝送網（ネットワーク）を通じて配信し、第２の暗号鍵を第２の伝送網（ネットワーク）を通じて配信する方法を採り得る。このように全ての鍵情報を伝送網を通じて配信すると、鍵情報の配信に要する時間的制約を少なくできる。また鍵情報の配信を経済的に実施できる。なお以上の伝送網（ネットワーク）を用いた鍵情報の配信に際しては、例えば電子証明書を使用して本人確認（配信先の確認）を行い、認証された配信先が公開する公開鍵で暗号化した鍵情報を配信するなどの手法が望ましい。

【００６８】また例えば、暗号化された第１の暗号鍵を第１の記録媒体を介して配信し、第２の暗号鍵を第２の記録媒体を介して配信する方法を採り得る。このように全ての鍵情報を有体物である記録媒体の形態で配信すると、鍵情報の盗難をより一層発見し易くでき、不正行為に対する対抗策をいち早く実施できる。勿論、２つの記録媒体には物理的に異なる媒体を使用する。言うまでもなく、記録媒体の種類や読み取り方式については同じでも、異なっても構わない。

【００６９】（２－４）第４の手段

第４の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【００７０】上流側システムがその制御下において、ディジタルデータを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の及び又はディジタルデータに固有の第２の暗号鍵を発生する処理と、上記第２の暗号鍵を基に一組の合わせ鍵を生成する処理と、第２の暗号鍵で暗号化された第１の暗号鍵又はその発生情報と上記第２の暗号鍵から生成された一組の合わせ鍵又はその発生情報をディジタルデータとは別の配信経路であって、相互においても別の配信経路となるものを用いて配信する処理と、暗号処理の施されたディジタルデータを配信する処理とを実行するものを提案する。

【００７１】また下流側システム（個々の配信先毎に設けられる。）では、正規の手続きによってのみ開封可能な復号サーバの制御下において、複数の配信経路を通じて配信を受けた一組の合わせ鍵又はその発生情報を基に第２の暗号鍵を復元して、配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、第１の暗号鍵を復元する処理と、復元された第１の暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理において生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力する処理とを実行するものを提案する。

【００７２】また正規の手続きによってのみ開封可能な出力装置の制御下において、上記復号サーバから入力されるディジタルデータに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行するものを提案する。

【００７３】第４の手段は要するに、第２の暗号鍵を例えば分割して一組（例えば３個）の合わせ鍵とし、それらを暗号化された第１の暗号鍵と共に配信する方式と、配信を受けた鍵情報から復元された暗号鍵を用い暗号処理の解除されたディジタルデータにスクランブル処理を施したものを出力装置に出力する再生方式とを組み合わせたものである。勿論、これら鍵情報の配信経路には、ディジタルデータとは別の配信経路であり、かつ各鍵情報相互間においても別の配信経路となるものを使用する。

【００７４】かかる第４の手段を用いれば、複数の配信経路を通じて配信される複数の鍵情報のうちいずれかが盗難されたとしても残る全ての鍵情報も盗難されない限り暗号鍵の流出を防止できる配信モデルを提供できる。しかもこの第４の手段の場合には、第３の手段よりも更に鍵情報の配信経路を増やせるため、より不正行為に対する安全性の高い配信モデルを提供できる。

【００７５】なお第２の暗号鍵から一組の合わせ鍵を生成するのに用いる方法としては、上述のように所定の分割規則で第２の暗号鍵を分割する方法の他、第２の暗号

鍵を更に別の暗号鍵で暗号化して得られる鍵情報とその暗号化に使用した暗号鍵をも含む。因みに、分割規則は全ての配信先に共通の規則でも良いし、各配信先に固有の規則でも良いし、特定地域その他の条件で区分された配信先の集合毎に固有の規則でも良い。またディジタルデータに固有の規則であっても良い。勿論、これら配信先についての規則とディジタルデータについての規則とを組み合わせることにより、より一段と鍵情報の流出し難いシステムを構築できる。

【００７６】なおこの第４の手段で用いる第２の暗号鍵も第３の手段と同様のものを使用する。例えば、第２の暗号鍵として配信先である各配信者に固有のものを用いる。この場合、特定の配信者から全ての鍵情報（第２の暗号鍵から生成された一組の合わせ鍵と、第２の暗号鍵で暗号化された第１の暗号鍵）を盗難しない限り、ディジタルデータに施されている暗号を解除できない。すなわち、第３の手段よりもある配信者に宛てて配信された固有の第２の暗号鍵が盗難される危険性を一段と低減できる。

【００７７】また第２の暗号鍵としてディジタルデータに固有のものを用いる場合には、全ての鍵情報が盗難された場合でもその被害を特定のディジタルデータ（勿論、暗号化されたディジタルデータも盗難されることが前提となる。）に限定できるのに加え、第２の暗号鍵が盗難される可能性自体をより一段と低下できる。

【００７８】なお言うまでもないが、第２の暗号鍵として配信先である各配信者について固有であり、かつディジタルデータについても固有のものを用いれば、より盗難の難しいシステムとできる。上述のいずれの暗号鍵を採用するかは、配信対象であるディジタルデータの経済的価値やディジタルデータの運用ポリシーによる。

【００７９】因みに第１の暗号鍵の暗号化は第２の暗号鍵で少なくとも１回行えば良く、他の種類の暗号鍵で暗号化する処理と組み合わせても良い。従って、第２の暗号鍵で暗号化する前に既に第１の暗号鍵が暗号化されていても良い。このような場合でも第１の暗号鍵が第２の暗号鍵で暗号化されていることに技術上の違いはない。

【００８０】なお第４の手段における鍵情報の配信方法としては、例えば次のようなものを採り得る。例えば、暗号化された第１の暗号鍵を記録媒体で配信し、第２の暗号鍵から生成された一組の合わせ鍵の一部を伝送網（ネットワーク）で配信し、残る部分鍵を記録媒体で配信する方法を採り得る。このように鍵情報の一部を記録媒体の形態で配信することで鍵情報の盗難を発見し易くでき、不正行為に対する対抗策をいち早く実施できる。なお言うまでもなく、記録媒体による配信はいずれの鍵情報でも良いし、任意の１種類の鍵情報を記録媒体で配信し、その他の鍵情報は伝送網（ネットワーク）を介して配信することもできる。

【００８１】また例えば、暗号化された第１の暗号鍵と、第２の暗号鍵から生成された一組の合わせ鍵の全てを伝送網（ネットワーク）を通じて配信する方法を採り得る。このように全ての鍵情報を伝送網（ネットワーク）を介して配信すると、鍵情報の配信に要する時間的制約を少なくできる。また鍵情報の配信を経済的に実施できる。なお以上の伝送網（ネットワーク）を用いた鍵情報の配信に際しては、例えば電子証明書を使用して本人確認（配信先の確認）を行い、認証された配信先が公開する公開鍵で暗号化した鍵情報を配信するなどの手法が望ましい。

【００８２】また例えば、暗号化された第１の暗号鍵と、第２の暗号鍵から生成された一組の合わせ鍵の全てを記録媒体を通じて配信する方法を採り得る。このように全ての鍵情報を記録媒体を介して配信すると、鍵情報の盗難をより一層発見し易くでき、不正行為に対する対抗策をいち早く実施できる。勿論、鍵情報の配信に使用する記録媒体はそれぞれ媒体の形態が異なっていても良いし、読み取り方式が異なっていても良い。

【００８３】

【発明の実施の形態】（１）ビジネスモデル

（１－１）一般例

図１に本願明細書が想定するビジネスモデルの基本的な構成例を示す。このビジネスモデルは、ディジタルデータの送り手である配信者と、ディジタルデータの受け手である特定者とで構成される。なお図１は、配信者が、ディジタルデータの配給権を有する配給権者１とディジタルデータの配信事業を行う配信事業者２の二者で構成される場合を表わしている。これは配給権者と配信事業者が同一人である場合も少なくないと考えられるが、それ以上に複数人によって配信者が構成される場合も少なくないと考えられるためである。

【００８４】また、配給権者１はコンテンツ制作者からコンテンツ、すなわちディジタルデータの配給権を譲り受けた者である場合の他、コンテンツ制作者自身である場合、配給権者とコンテンツ制作者の共同事業体の場合もある。他方、特定者には個人や事業者（例えば劇場事業者）が該当する。

【００８５】上述したように、ここでは上流側システム（データの流れから見て上流側のシステムの意味）が配給権者のシステムと配信事業者のシステムで構成され、下流側システム（データの流れから見て下流側のシステムの意味）が特定者のシステムで構成される場合について説明する。

【００８６】配信対象に想定するディジタルデータは、文字データ（例えば、テキスト、記号、図形）、オーディオデータ（例えば、音声、楽曲）、ビデオデータ（例えば、静止画、動画）、オーディオデータとビデオデータの複合データ（例えば、映画、放送番組）、プログラムデータ、データベースデータ、その他のディジタルデータがある。勿論、これらの付属情報（例えばメタデー

タと呼ばれるＩＤ（媒体上の識別情報）、撮影日時、場所、人物、状態等に関する情報がある。）も含まれ得る。

【００８７】一般に、ディジタルデータの配信には、伝送帯域が広く大容量のデータを配信するのに適した高速配信用ネットワーク３を想定する（図１）。この図１においては、コンテンツ制作会社１から電子配信事業者２にコンテンツとしてのディジタルデータを送り、高速配信用ネットワーク３を介して、特定者Ａ，Ｂ等にディジタルデータを配信するシステムを示している。ただし、ＣＤ－ＲＯＭやＤＶＤその他の記録媒体による形態での配信を排除するものではない。高速配信用ネットワーク３には、放送衛星や光ファイバその他の広帯域伝送網を使用する。これらは少なくとも下り方向について大容量の伝送が可能なものを使用する。もっとも、上り方向への伝送も可能な双方向伝送網を用いても良い。

【００８８】高速配信用ネットワーク３には、図２に示したようなデータ構造のデータ８が配信される。ここで、図２のデータ８には鍵の絵８Ａを表しているが、これはネットワーク提供者（配信事業者でない）が自身の提供する通信サービスの秘匿性を確保するために独自に暗号鍵を掛ける場合を表している。従って、この鍵は掛けられない場合もある。

【００８９】もっとも、ディジタルデータの不正行為に対する安全性を最優先する配給権者や配信事業者は、ネットワーク上でも独自にデータに暗号処理を施すネットワーク事業者を選択するであろうし、その中でもより安全性の高い暗号処理を実行するネットワーク事業者を選択するものと考えられる。なお図２においては省略しているが、実際にはデータ８を配信する上で必要なヘッダが存在する。

【００９０】図２の破線で囲まれた中身の部分が上記電子配信事業者２から配信されるデータに相当する。図２の場合、当該データには、データ又はファイルの格納情報を示すファイルアロケーションテーブル（ＦＡＴ：File Allocation Table）８Ｂと、ディジタルデータの使用条件（配信先、配信先毎の再生可能期間及び再生回数その他の条件）を含む業務データ８Ｃと、映像データ８Ｄと、音声データ８Ｅとが格納されている。

【００９１】ここで各データに掛けられている鍵の絵は、これら各データが配給権者や配信事業者（そのいずれかの一方によって、又はその両者の協動によって）の施した暗号処理によって保護されていることを表わしている。ここで、各データに施されている暗号鍵は一般に同じ暗号鍵が使用される。ただし、データの種別ごと（例えば映像データごと）に異なる暗号鍵を採用しても良いし、データの種別に係わらず各データごと（例えば、コーデックを異にする映像データや音声データごと）に異なる暗号鍵を掛けることも可能である。

【００９２】図２に示すように、この配信モデルでは、あるコンテンツをマルチフォーマットで配信する方式を採用する。すなわち、配信対象である１つのコンテンツについて符号化復号化方式（コーデック）を異にする複数種類の映像データや音声データを用意して配信する方法を採用する。図２の場合、ある映像コンテンツについてコーデック方式を異にする３種類の映像データが配信される様子を表している。ここでのコーデック方式としては、例えば、ＭＰＥＧ（Moving Picture Experts Group）、ウェイブレット（Wavelet）その他が考えられる。

【００９３】このように映像コンテンツを複数種類のコーディック方式で符号化し配信するのは、配信を受ける特定者側のシステム構成に自由度をもたせるためである。これにより、特定者はディジタル配信サービスの利用のためだけに専用のコーデックシステムを採用せずに済み、自身の使い慣れたシステムをそのまま利用することができる。このように、マルチフォーマットによる配信方式は、配信者の側から見ると特定者（データの配信先）が特定のシステムを保有するものに限られない利点があり、特定者の側から見るとディジタルデータの選択範囲が限られないため既存の設備を有効活用できる利点がある。

【００９４】音声データ８Ｅについても同様である。図２の場合、２種類のコーデック方式で符号化されたデータが格納されている。ここでのコーデック方式には、例えば、ＭＰＥＧその他がある。

【００９５】なお図１のビジネスモデルの場合、特定者Ａと表した個人宅が受信可能なデータは、映像コーデック$VCD_1$で符号化された映像データと音声コーデック$ACD_1$で符号化された音声データであるため、それらが配信を受けたデータ８の中からＦＡＴの情報を基に選択的に抽出される又は再生される。一方、特定者Ｂと表した事業者が必要とするデータは、映像コーデック$VCD_2$で符号化された映像データと音声コーデック$ACD_2$で符号化された音声データであるため、それらが配信を受けたデータ８の中からＦＡＴの情報を基に選択的に抽出される又は再生される。もっとも常にマルチフォーマットで配信しなければならないわけではないし、配信先毎に必要とされるフォーマットの組み合わせの情報を配信しても良い。

【００９６】以上が高速配信用ネットワーク３を介して配信を受けるディジタルデータについての説明である。次に、当該ディジタルデータに施されている条件付きアクセス処理（Conditional Access）、すなわちディジタルデータに施されている暗号処理を解除するのに必要な暗号鍵の配信経路について説明する。図１では、暗号鍵の配信経路として、広域ネットワーク（伝送媒体）４と記録媒体５の２つを用いている。すなわち、図１は、共通鍵を復元するのに少なくとも２種類の鍵情報を必要とする場合において、その一部を広域ネットワーク４を介

して電子的に配信し、残る一部を記録媒体５を通じて物理的に配信する方式を採用する配信方式の一例を表わしている。

【００９７】なお、ここでの広域ネットワーク４は双方向通信が可能な伝送網を想定している。例えば、公衆網（例えば、インターネット網、ＡＴＭ網、パケット通信網）や専用線網が考えられる。また、記録媒体５は前述の課題を解決するための手段にて述べたように、磁気読み取り方式の媒体、光学読み取り方式の媒体、半導体メモリその他を想定する。その配信に郵便制度や宅配制度を利用することも前述の通りである。

【００９８】なお以下の説明では、ディジタルデータに施す暗号鍵は全ての配信先について共通であり、各配信先に個別に配信される一組の鍵情報は各特定者に固有であると想定する。これは特定者毎に固有の鍵情報を採用することで、ある特定者に宛てて配信された全ての鍵情報を入手しない限り、ディジタルデータに掛けられている暗号鍵を復元できないようにするためである。このような仕組みを採用することで、このビジネスモデルは、全ての鍵情報を不正に入手するのがより困難なもの又は全ての鍵情報を不正に入手するのに時間を要するものとできる。

【００９９】因みに前述の場合には、各ディジタルデータの暗号化に使用する暗号鍵を全配信者に共通なものとしたが、各ディジタルデータの暗号化に使用する暗号鍵を各配信先毎に固有のものとすることもできる。また前述の場合には、各配信先に個別に配信される一組の鍵情報が各配信先に固有のものとしているが、各ディジタルデータに固有のものとすることもできる。

【０１００】因みに、ディジタルデータに掛けられる暗号鍵は、配信対象であるコンテンツに固有なものであることが望ましい。これは前述のように全ての鍵情報が不正に流出しディジタルデータの復号に成功したとしても被害を特定のコンテンツに限定できるためである。勿論、当該暗号鍵がコンテンツ毎に固有であることは必須ではなく、複数のコンテンツについて共通の暗号鍵を使用することも考えられる。要はシステム全体として不正行為に対する秘匿性が高まれば良いのであって、個々の暗号鍵が特定の規則に限定されるものではない。また秘匿性の高さは配信対象であるコンテンツによっても異なり、配信者側のポリシーによっても異なる。

【０１０１】次に配信経路について説明する。基本的に鍵情報の配信には、図１に示すように、ネットワークと記録媒体というように媒体を異にするものを想定する。これは各配信経路の有する以下の特質に基づくものである。

【０１０２】まず、ネットワークの場合、鍵情報の配信を即時に実行できるという利点を有する。ただし、鍵情報が盗難された場合に発見が難しいという欠点がある。これに対し、記録媒体の場合、鍵情報の配信は特定者が入手するまでに所定の時間を要するという欠点を有するが、鍵情報の盗難を物理的に確認することができるため盗難を発見し易いという利点がある。

【０１０３】そこで、本願明細書で想定する多くのビジネスモデルでは、ネットワークを介しての配信と、記録媒体による物理的な配信との組み合わせを想定する。もっとも以上一般的な理由によるものであり、ネットワークを使った配信でも不正行為のおそれがない場合や困難な場合には、全ての鍵情報をネットワークを介して配信すればよい。また、鍵情報の配信からディジタルデータの配信までに期間的な余裕がある場合には、鍵情報の全てを記録媒体を使用して配信することもできる。

【０１０４】因みに、ディジタルデータの暗号処理に使用する暗号技術については技術的な制約はなく、出願当時知られている各種の技術は勿論のこと将来現れるであろう各種の技術についても適用できる。暗号方式を問わないため技術的な寿命の影響を受け難いビジネスモデルとできる。また、常に運用当時最高の技術を選択できるため、その分、不正行為に強いビジネスモデルとできる。

【０１０５】また図１において広域ネットワーク４と記録媒体５との２つの経路を通じて配信される鍵情報は、課題を解決するための手段において説明したように、配信先毎に固有の分割パターンで分割された一組の合わせ鍵（部分鍵）の組、又は、配信先毎に発生された固有の多重鍵で暗号化された暗号鍵と多重鍵の組を一般には想定する。

【０１０６】（１－２）具体例

図３に、具体的なビジネスモデル例を示す。これは映画コンテンツを電子的に配信するビジネスモデルについてのものである。この種のビジネスモデルは従来からその実現に向け各種のビジネスモデル案が提供されているが、映画コンテンツの配給権を有する事業者と配信を受ける劇場側の双方を十分に満足させるものはなく実用に至ったものはない。そこで、本願明細書の配信モデルを適用することを考える。

【０１０７】この図３に示すビジネスモデルの場合、図１のコンテンツ制作会社１は映画製作会社１ａに変わり、ディジタルデータの配信を受ける特定者６，７は劇場Ａ、Ｂに変わる。なお、図３の場合、映画コンテンツに特有な構成として、映画製作会社１ａから提供されるフィルム画像を電子画像に変換する工程（テレシネ工程：Film to Video Conversion）９を表している。また図では区別していないが、劇場Ａ、Ｂは大規模な映画館や、小規模な映画館や、いわゆるシネコンと呼ばれる映画館等が想定される。

【０１０８】（２）配信システム例

上述のビジネスモデルを実現する配信システムの機能ブロック構成例を示す。なお各システム例は、課題を解決するための手段で説明した第１～第４の手段のいずれか

に対応する。勿論、実施形態例であるから部分的には特定の機能に限定した記載もあるが、前述の通りこれらに限られるものではない。

【０１０９】（２－１）第１の配信システム例

図４に、上述のビジネスモデルを実現するための第１の配信システム例を示す。なお第１の配信システム例は前述の第１の手段に対応する。当該システムは上流側システムと下流側システムとで構成される。ここでの上流側システムは、コンテンツの配給権を有する事業者１のシステムと電子配信事業者２のシステムの複合システムとする。勿論前述のように単一事業者のシステムを排除するものではないし、３者以上の事業者による複合システムを排除するものではない。一方、下流側システムはディジタルデータの配信を受ける特定者毎に固有のシステムとする。

【０１１０】（２－１－１）概念構成

まず当該第１の配信システム例の概念構成を説明する。この第１の配信システムには、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。

【０１１１】（１）第１のモデル

第１のモデルとして見た上流側システムは、各ディジタルデータに固有の暗号鍵を発生する処理と、ディジタルデータを対応する暗号鍵で暗号化する処理と、上記暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部を伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵又はその発生情報のうち残りの部分を記録媒体の形態での配信用に鍵専用の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。

【０１１２】一方、下流側システムは、伝送網を通じて配信を受けた合わせ鍵又はその発生情報の一部と記録媒体の形態で配信を受けた残りの部分とを基に対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理とを実行する。

【０１１３】第１のモデルは要するに、ディジタルデータの暗号化に使用した暗号鍵を、各配信先（下流側システム）に固有の分割規則で分割して一組の合わせ鍵を生成し、その一部を伝送網を通じて配信し、残りを記録媒体の形態で配信する方式を採用するものである。

【０１１４】（２）第２のモデル

第２のモデルとして見た下流側システムの復号サーバは、伝送網を通じて配信を受けた合わせ鍵又はその発生情報の一部と記録媒体の形態で配信を受けた残りの部分とを基に対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。

【０１１５】このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを採用する。

【０１１６】第２のモデルは要するに、配信を受けた鍵情報から復元された暗号鍵を用い暗号処理の解除されたディジタルデータにスクランブル処理を施して出力装置に出力する再生方式を採用するものといえる。

【０１１７】なお、復号サーバで生成するスクランブル鍵とスクランブル解除鍵は、同じディジタルデータについては同じであっても良いし、暗号処理を解除する毎に固有の鍵を発生するようにしても良い。不正行為に対する対策としては後者の方が望ましい。

【０１１８】また、出力装置としては表示装置（例えば、モニタ装置、テレビジョン受像機、プロジェクタ装置、携帯型の電子機器）、印刷装置、スピーカ、記録媒体への記録装置等が考えられる。

【０１１９】ここで、出力装置における所定の出力形態には、ディジタルデータが例えばビデオデータであれば、表示画面への表示、投影面への投影が考えられる。またディジタルデータが例えばオーディオデータであれば、スピーカを通じての再生が考えられる。勿論、オーディオデータとビデオデータの複合データであれば、その同時に２つの出力が行われる。

【０１２０】なお、以上の復号サーバや出力装置には、いわゆる完成品の他、該当機能を実現する回路装置（例えば、インタフェースボードや半導体集積回路等）のような構成部品も含まれる。

【０１２１】（２－１－２）システム構成

図４の場合、上流側システムは、コンテンツサーバ１１と、コンテンツ符号化部１２と、暗号化部１３と、送出サーバ１４と、コンテンツ管理サーバ１５と、鍵発生部１６と、配信先管理サーバ１７と、合わせ鍵生成部１８と、書込部１９とから構成される。

【０１２２】図４では、上流側システムにおけるこれらの各構成要素がいずれの事業者内システムに設けられるかをあえて明示していないが、これは各構成要素を各事業者にどのように配分するかはビジネス上の選択となるためである。なお各構成要素の配分又は配置の仕方は、

他のシステム例についても共通する事項であるため、後段の「各システムで想定される運用形態」の項で別途説明する。

【０１２３】一方、下流側システムは、受信サーバ３１と、読取部３２と、復号サーバ３３と、出力装置３４（デスクランブル部３４Ａ）とから構成される。このうち、復号サーバ３３は、更に復号機能部３５（復号化部３５Ａ、鍵復元部３５Ｂ、コンテンツ復号化部３５Ｃ、スクランブル部３５Ｄ）と、スクランブル制御部３６と、出力ログ管理部３７とで構成される。

【０１２４】なお、これらの各構成要素はそれぞれ専用のハードウェアとして実現することも可能であるし、ソフトウェアの一機能として実現することも可能である。

【０１２５】また図中、太線で示す矢印は伝送容量の大きい伝送路を表しており、細線で示す矢印は伝送容量の比較的小さい伝送路を表している。もっとも現時点で想定されるシステム構成であり、伝送容量が大きいか小さいかは相対的なものである。また現時点では細線の矢印で示す合わせ鍵の配信経路も伝送容量の大きいものとしても良い。

【０１２６】（２－１－３）各機能部の構成

まず、上流側システムを構成する各機能部を説明する。

コンテンツサーバ１１は、記録媒体（図４では磁気テープ）や伝送路を通じて提供を受けたディジタルデータの蓄積を主な機能とする装置である。このため大容量のストレージ装置を備える。なお当該サーバはコンピュータ構成を採る。

【０１２７】すなわち、当該サーバは、制御機能と演算機能を実現する処理装置と、信号処理の実行に必要なデータを記憶する記憶装置と、外部からデータやプログラム及びコマンドを入力する入力装置と、処理結果を外部に出力する出力装置とを備える構成を採る。

【０１２８】コンテンツ符号化部１２は、ディジタルデータの圧縮符号化その他の符号化処理を主な機能とする装置である。例えば、ＭＰＥＧ変換やＷａｖｅｌｅｔ変換その他の符号化処理が実行される。なお、符号化処理は一般に１種類だけが行われるのではなく、運用時に広く採用されている複数の符号化処理が行われる。この結果、１つのディジタルデータに対して複数の符号化処理データが生成される。なお音声や画像データに透かし情報を埋め込む処理は、例えばコンテンツサーバ１１とコンテンツ符号化部１２との間で実行される。このコンテンツ符号化部１２は、専用のハードウェアを用いて構成しても良いし、当該ハードウェアと同等の機能を実現させるプログラムがインストールされているコンピュータのソフトウェア上の処置として実現しても良い。

【０１２９】暗号化部１３は、鍵発生部１６からコンテンツに固有の暗号鍵の提供を受け、当該暗号鍵を用いてコンテンツ符号化処理の終了したディジタルデータに暗号処理を施す装置である。ここで使用する暗号方式は運用時に広く採用されているものを用いれば良い。

【０１３０】例えば、ＤＥＳ（Data Encryption Standard）、ＦＥＡＬ（Fast Data Encipherment Algorithm）その他の暗号処理が実行される。ここでの暗号処理は、業務データとコンテンツデータのそれぞれについて個別に実行される。参考までに言及すると、コンテンツデータについての暗号処理は、コンテンツ符号化部１２で生成された各符号化データ毎に実行される。

【０１３１】なお暗号化部１３も、専用のハードウェアを用いて構成してもよいし、コンピュータに同等の機能を実現させるソフトウェアの処理機能として実現してもよい。

【０１３２】送出サーバ１４は、特定者のみが視聴又は記録できるように暗号化処理の施された（条件付きアクセス処理が施された）ディジタルデータをストレージ装置に蓄積する機能と、配信スケジュールに従って高速配信用ネットワーク３に出力する機能とを実現する装置である。ここでの出力機能は、広帯域伝送機能やレートコントロール機能を備える送信装置で実現される。

【０１３３】高速配信用ネットワーク３を用いたデータの配信は現在のところ夜間を利用した蓄積型の配信を想定しているが、伝送速度の向上が期待される将来においてはストリーミング配信等も想定する。

【０１３４】なお、ディジタルデータの配信を記録媒体の形態で実行する場合、前述した出力機能はディジタルデータを所定の記録媒体に格納する記録装置で実現される。

【０１３５】コンテンツ管理サーバ１５は、コンテンツサーバ１１と通信し、新たに受付けたコンテンツの登録処理やコンテンツの検索処理、ファイル分割処理その他を実行する装置である。当該サーバもコンピュータ構成を採る。当該サーバではコンテンツ毎に発生された暗号鍵情報が管理される。例えば、コンテンツと対応する暗号鍵との関係がデータベースとして管理される。

【０１３６】鍵発生部１６は、配信対象であるディジタルデータ毎に固有の暗号鍵を生成する手段である。暗号鍵の発生に使用される暗号方式は運用時に広く採用されているものを使用する。すなわち、不正な解読が困難な最新の暗号化技術に従う。

【０１３７】配信先管理サーバ１７は、コンテンツ毎に配信先と配信条件その他の業務データや配信先毎に生成した暗号鍵の情報をデータベースにより管理する装置である。ここでの配信条件には使用可能期間、出力可能回数その他の情報が含まれる。また当該サーバもコンピュータ構成を採る。

【０１３８】配信先管理サーバ１７は、コンテンツ配給権者１のシステムにのみ設ける場合、電子配信事業者２のシステムにのみ設ける場合、両者のシステム内に設ける場合その他が考えられる。これは各配信先に固有の鍵情報を誰が配信するかはビジネス上の選択事項だからで

ある。ただし、鍵情報を知り得る事業者は少ないほどシステム全体からみた秘匿性は高まることは言うまでもない。一般にはコンテンツ配給権者１のシステム内に配置されるものと思われるが、ビジネスの運営形態に応じて電子配給事業者その他の事業者のシステム内に配置される場合もあり得る。

【０１３９】図４その他の図面における配信先管理サーバ１７は、下流側システムの出力ログを上り回線（一般にはインターネットや電話回線その他の通信回線を使用する。）を通じて受信できるように構成されている。配信先管理サーバ１７は、当該出力ログに基づいて配信先（受信者側）の出力履歴（出力日時、出力回数、期間、付帯情報（トラブルの有無、コンテンツ視聴者の数や年齢層など）その他）を管理する。このため、配信先管理サーバ１７は、不図示のデータベースや出力履歴管理機能部を備える。

【０１４０】もっとも、これらデータベースや出力履歴管理機能部は、配信先管理サーバ１７と別に設けられていても良い。なお出力ログの集計処理（統計処理も含む。）や分析処理は、出力ログの通知を受けた上流側システムにて実行しても良いし、下流側システムが予め実行した結果を送信するものとしても良い。

【０１４１】このように下流側システムの出力ログ（実行事実）を上流側システムで管理することにより、コンテンツの流通状況を監視可能とできる。また、市場動向（興行成績、流行、傾向その他）を把握するのに使用できる。もっとも、ここでの上流側システムは広義の上流側システムであり、ディジタルデータの配信権を有する事業者や電子配信事業者以外の事業者、例えばコンテンツの出力動向を調査する事業者であっても良い。

【０１４２】なお、出力ログの受信は配信先管理サーバ１７が行わなくても良く、他の電子機器で受信しても良い。またここでの出力ログは、前述した全ての情報（例えば出力日時等）を表示する必要はなく、任意の１つ又は任意の組み合わせが通知されていても良い。ところで、図４を始め各図においては出力ログを下流側システムから上流側システムへ通知する場合を表わしているが、常に通知する必要はなく、また出力ログの通知を行わない配信システムを考えることも可能である。

【０１４３】合わせ鍵生成部１８は、コンテンツ毎に生成された暗号鍵Ａを配信先毎に固有の分割パターンで分割し、一組の合わせ鍵Ａ１及びＡ２を生成する装置である。例えば、配信先となる特定者が１０００人いれば、１０００組の合わせ鍵Ａ１及びＡ２が生成される。生成された合わせ鍵は、合わせ鍵生成部１８によって配信先管理サーバ１７と所定の配信処理部に与えられる。このシステムの場合、合わせ鍵生成部１８は、合わせ鍵Ａ１をネットワークを介した配信用に不図示の通信部に与え、残る合わせ鍵Ａ２を記録媒体を介した配信用に書込部１９に与える。

【０１４４】書込部１９は、通知を受けた合わせ鍵Ａ２を所定の記録媒体に書き込むための装置である。書込部１９には、記録媒体に応じた駆動機構が設けられる。記録媒体には、磁気読み取り方式の媒体、光学読み取り方式の媒体、半導体メモリその他の媒体が用いられる。なお、記録媒体の配信に必要な宛先情報は配信先管理サーバ１７から与えられる。前述の不図示の通信部についても同様である。ただし、通信部の場合にはネットワーク上のアドレスが与えられる。

【０１４５】次に、下流側システムを構成する各機能部を説明する。受信サーバ３１は、特定者のみが視聴又は記録できるように暗号化処理の施された（条件付きアクセス処理が施された）ディジタルデータの受信機能と、配信を受けたディジタルデータをストレージ装置に蓄積する機能と、再生スケジュールに従って復号サーバ３３に出力する機能とを実現する装置である。ここでの受信機能は、受信データに含まれる誤り訂正等を行う機能も備える。

【０１４６】なお、ディジタルデータの配信を記録媒体の形態で受ける場合、前述した受信機能はディジタルデータを所定の記録媒体から読み取る読取装置で実現される。

【０１４７】読取部３２は、記録媒体の形態で配信される合わせ鍵Ａ２を記録媒体から読み取るための装置である。ここで駆動機構には、記録媒体に応じたものが用いられる。また、図中では表していないが、広域ネットワークを介して配信を受ける合わせ鍵Ａ１の受信用に通信部が設けられている。

【０１４８】復号サーバ３３は、ディジタルデータに施されている暗号処理を解除する処理と、暗号が解除されたディジタルデータに施されている符号化処理を復号化する処理とを実行する一方で、復元された生のディジタルデータがそのまま装置外部に出力されないように局所的なスクランブル処理を施す装置である。

【０１４９】復号サーバ３３は、専用のハードウェアを用いて構成しても良いし、コンピュータに同等の機能を実現させるソフトウェアの処理機能として実現しても良い。因みに当該復号サーバ３３は、悪意の特定者による不正行為からディジタルデータを保護するため、正規の手続き以外ではその筐体を開封できない仕組みや不正に開封すると動作しなくなる仕組みを採用する。これらの仕組みについては既存の技術を使用する。

【０１５０】特に、復号機能部３５（復号化部３５Ａ、鍵復元部３５Ｂ、コンテンツ復号化部３５Ｃ、スクランブル部３５Ｄ）については、各機能ブロック間において重要な情報（暗号鍵や生のディジタルデータ）が流れるため、不正行為を排除するための対策が重要であり、当該機能ブロック部分を半導体集積回路化したり、正規な手続き以外ではその筐体を開封できない仕組みや不正に開封すると動作しなくなる仕組みを採用する。

【０１５１】ここで、復号化部３５Ａは、鍵復元部３５Ｂから与えられる暗号鍵を用い、受信サーバ３１から読み出されたディジタルデータに施されている暗号処理（条件付きアクセス処理）を解除する機能部である。当該機能は専用のハードウェアで実現することもできるし、ソフトウェア上の機能として実現することもできる。

【０１５２】鍵復元部３５Ｂは、ネットワークを介して配信を受けた合わせ鍵Ａ１と記録媒体の形態で配信を受けた合わせ鍵Ａ２に基づいて、ディジタルデータに施されている暗号処理を解除できる暗号鍵を復元する機能を実現する機能部である。復元された暗号鍵は鍵復元部３５Ｂの管理下において所定の期間保持される。当該確認には不揮発性メモリ、ハードディスクその他の記録媒体が用いられる。

【０１５３】また鍵復元部３５Ｂは、受信サーバ３１から読み出されたディジタルデータの暗号を復号するのに先だって、当該ディジタルデータに付属されている業務データ８Ｃを読み出し、当該業務データ８Ｃで定められている再生条件（使用条件）が各時点において満たされているか否かの判定も行う。

【０１５４】ここで、鍵復元部３５Ｂは、再生条件が満たされるとき、復号化部３５Ａに暗号解除許可信号を与える一方、スクランブル制御部３６にスクランブル鍵の発生信号又は出力許可信号を与える。これに対し、鍵復元部３５Ｂは、再生条件が満たされないとき、復号化部３５Ａに暗号解除禁止信号を与えると共に、スクランブル制御部３６にスクランブル鍵の発生禁止信号又は出力禁止信号を与える。

【０１５５】コンテンツ復号化部３５Ｃは、特定者毎が採用しているコーデック方式に対応するものが用いられる。当該機能も専用のハードウェアとして実現することも可能であるし、ソフトウェアの一機能として実現することも可能である。コンテンツ復号化部３５Ｃの信号処理の結果、暗号化処理前の生のディジタルデータが復元される。

【０１５６】スクランブル部３５Ｄは、コンテンツ復号化部３５Ｃによって復元されたディジタルデータがそのままの形態で出力されることがないように、スクランブル処理を施すための装置である。当該機能も専用のハードウェアとして実現することも可能であるし、ソフトウェアの一機能として実現することも可能である。

【０１５７】なお図４の場合、スクランブル制御部３６を復号機能部３５の外部においているが、スクランブル制御部３６を復号機能部３５内の一機能として設けることも可能である。

【０１５８】スクランブル制御部３６は、鍵復元部３５Ｂによりスクランブル鍵の発生が許可された場合、スクランブル鍵とこれと対をなすデスクランブル鍵を発生する。なお鍵復元部３５Ｂからスクランブル制御部３６に与えられる許可信号は、単なる許可と非許可の情報だけでなく、出力日時や期間等の情報を含むものでも良い。またスクランブル制御部３６を図中破線で示すように、コンテンツ復号化部３５Ｃその他に対して外部接続する場合には当該機能部間で互いを認証し、相手側が真正であると認めた場合にのみスクランブル鍵が発行されるようにしても良い。

【０１５９】なお、スクランブル鍵とデスクランブル鍵の発生方法には、コンテンツの違いによらずいつも同じスクランブル鍵等を発生する方法（固定的に記憶されているスクランブル鍵とデスクランブル鍵を出力する方法）と、コンテンツ毎に異なるスクランブル鍵等を発生する方法（新たなコンテンツの出力のたび生成され、所定の再生条件が満たされる間保持される方法）と、再生出力のたびに異なるスクランブル鍵等を生成する方法（コンテンツの暗号を解除するたびに異なるスクランブル鍵を生成する方法）とがある。不正行為に対する防御機能の観点からは、記載順に３番目の方法、２番目の方法、１番目の方法の順番で不正が困難になる。

【０１６０】因みに、スクランブル制御部３６は、１つのコンテンツを出力する間にスクランブル鍵を定期又は不定期に切替える仕様を採用する場合にはディジタルデータの出力装置３４への出力中も適宜スクランブル鍵とデスクランブル鍵を発生する。

【０１６１】また図４その他の図面では、スクランブル制御部３６から出力ログ管理部３７にスクランブル鍵等の発生状況を通知するように描かれていないが、かかる管理情報を出力ログ管理部３６に与えるようにしても良い。このような情報を出力ログ管理部３７に与えることで、スクランブル鍵等が不正に発生されたものか否かを監視できる。

【０１６２】出力ログ管理部３７は、出力装置３４からの不正出力を監視するため、出力装置３４における出力ログを管理する装置である。当該機能も専用のハードウェアとして実現することも可能であるし、ソフトウェアの一機能として実現することも可能である。出力ログ管理部３７は、出力ログを通信回線を通じて上流側システムを構成する配信先管理サーバ１７に通知する。この結果、上流側システムでも別途、各特定者の再生出力状況を監視できる。また不正行為の発見にも利用できる。

【０１６３】なおここでの出力ログは、下流側システムで発生した又は入力された生のデータを想定しているが、当該出力ログ管理部３７その他の装置において集計処理（統計処理）や分析処理されたものでも良い。因みに、出力ログの情報としてコンテンツ視聴者の数や年齢層などの付帯情報を含める場合には、当該情報が不図示の入力手段や処理装置から与えられるものとする。

【０１６４】最後に、出力装置３４の構成を説明する。出力装置３４は、ディジタルデータに応じたものが用いられる。画像系であれば表示装置や投影装置が考えられ

るし、音声系であればスピーカーが考えられる。いずれにしても、出力装置３４は、その本来の機能部の他にデスクランブル部３４Ａを備える。

【０１６５】デスクランブル部３４Ａは、復号サーバ３３から与えられるディジタルデータに施されているスクランブル処理を解除するための機能装置である。当該機能も専用のハードウェアとして実現することも可能であるし、ソフトウェアの一機能として実現することも可能である。当該デスクランブル部３４Ａは、半導体集積回路やボード部材で構成される。

【０１６６】この出力装置３４の場合も、デスクランブル部３４Ａから出力される信号については、電子透かしのような静的な保護機能しか施されていないため、正規の手続き以外では出力装置の筐体を開封できない仕組みや不正に開封すると動作しなくなる仕組みを採用する。

【０１６７】（２－１－４）ディジタルデータの配信動作

第１の配信システム例におけるディジタルデータの配信動作を簡単に説明する。当該システムでは、新たなディジタルデータがコンテンツサーバ１１に登録されると、コンテンツ管理サーバ１５の管理下において当該コンテンツに固有の暗号鍵が発生される。次に、作成された暗号鍵が合わせ鍵生成部１８に与えられ、各配信者に固有の分割パターンによって固有の合わせ鍵が生成される。

【０１６８】ここで、各配信者に固有の分割パターンはコンテンツの違いにかかわらず同じものでも良いし、コンテンツ毎に異なる分割パターンを採用しても良い。いずれにしても、図４のシステム例では、特定者毎にコンテンツに固有の合わせ鍵が生成される。

【０１６９】その後、生成された合わせ鍵Ａ１とＡ２がディジタルデータの送信に先立って事前に配信される。このシステムの場合、合わせ鍵Ａ１はネットワークを通じて、合わせ鍵Ａ２は記録媒体に記録された形態で配信される。もっとも、常にディジタルデータの配信に先立って行われなければならない訳ではない。暗号処理の解除に必要な鍵がディジタルデータの配信後に行われる場合もあり得る。

【０１７０】ディジタルデータと合わせ鍵の配信を受けた下流側システムが、所定の出力スケジュールに従ってディジタルデータを読み出し、復元された暗号鍵で暗号処理を解除する。その後、暗号処理の解除されたディジタルデータのうち特定者のシステム構成に適合するコーデック方式にかかるものが選択的に復号化され、復号結果についてのスクランブル処理が復号サーバ３３にて実行される。

【０１７１】この後、復号サーバ３３からはスクランブル処理が施されたディジタルデータが出力装置３４に出力される。出力装置３４では、スクランブル制御部３６から与えられるデスクランブル鍵によってスクランブル処理の解除が行われ、所望の形態でコンテンツの出力が行われる。なおこの出力状況が出力ログとして出力ログ管理部３７より上流側システムに通知される。ここでの通知は、コンテンツの出力毎に行われても良い（すなわち、１回の出力に付き１回通知されても良い）し、複数回の出力情報をまとめて通知しても良い（例えば、１日毎に出力状況リストを出力しても良い）。

【０１７２】（２－１－５）第１の配信システム例によって得られる効果

上述のように第１の配信システム例によれば、合わせ鍵の配信経路を複数としたことにより、たとえいずれかの合わせ鍵が盗難されたとしても他方も盗難されない限り暗号鍵の流出を防止できる配信モデルを提供できる。特に、合わせ鍵をディジタルデータとは別の経路（上述のように同一の伝送媒体を用いながら時間的に別の時点に配信する場合を含む。）で配信する場合には、合わせ鍵の一部を盗んだ不正行為者が暗号化されたディジタルデータをも入手した場合でも、暗号鍵の復元に必要な鍵情報はディジタルデータとは別に配信されるため、生のディジタルデータが復号化される事態を確実に回避できる。

【０１７３】また暗号処理が解除されたディジタルデータにスクランブル処理を施す方式を採用したことにより、不正行為に対する十分な防御能力を保持したままで復号機能を実行するサーバ装置と再生機能を実行する出力装置との分離を実現できる。

【０１７４】特に、運用後により安全性が高い暗号方式が出現した場合や取り扱うコーデック方式を変更したい場合でも、復号サーバ３３のみを置き換えることで対処できる。また、特定者が取り扱うコーデック方式が何であったとしても、復号サーバ３３から出力装置３４に出力されるデータはスクランブル処理されたデータに統一されるため、出力装置３４を複数のコーデック方式で共用できる。

【０１７５】このことは出力装置３４の開発費が少なく済むことをも意味する。すなわち、汎用型の出力装置３４にデスクランブル部３４Ａを搭載するとともに、正規な手続きでしか開封できないか又は動作しない仕組みを搭載するだけでよいため、出力装置３４の低価格化を実現できる。従って、運用後により性能の高い出力装置が開発された場合でも、例えば再現解像度の高いものが開発された場合でも、装置の置き換えが進み易い。

【０１７６】かくして、不正行為に対する安全性もシステムを運用する上での経済性も同時に満足できる。

【０１７７】（２－２）第２の配信システム例

図５に、上述のビジネスモデルを実現するための第２のシステム例を示す。ここで図５は、図４との対応部分に同一符号を付して表したものである。図５と図４を対比して分かるように、当該システムを構成する下流側システムは第１の配信システム例と同じである。なお第２の配信システム例は前述の第２の手段に対応する。

【０１７８】（２－２－１）概念構成
まず当該第２の配信システム例の概念構成を説明する。この第２の配信システムの場合も、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。
【０１７９】（１）第１のモデル
第１のモデルとして見た上流側システムは、各ディジタルデータに固有の暗号鍵を発生する処理と、ディジタルデータを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、生成された部分鍵の一部又はその発生情報を第１の伝送網を通じて各特定者に配信する処理と、生成された部分鍵の残りの部分又はその発生情報を記録媒体の形態での配信用に鍵専用の記録媒体に書き込む処理と、部分鍵の生成に用いなかった残りの合わせ鍵又はその発生情報を第２の伝送網を通じて特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。
【０１８０】一方、下流側システムは、第１の伝送網を通じて配信を受けた部分鍵又はその発生情報と、記録媒体の形態で配信を受けた部分鍵又はその発生情報と、第２の伝送網を通じて配信を受けた合わせ鍵又はその発生情報を基に対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理とを実行する。
【０１８１】ここで、合わせ鍵から一組の部分鍵を生成するのに用いる分割規則は、全ての配信先に共通の規則でも良いし、各配信先に固有の規則でも良いし、特定地域その他の条件で区分された配信先の集合毎に固有の規則でも良い。他の手段においても同様である。
【０１８２】なおここでは、合わせ鍵の一部を更に分割して配信用の鍵情報を生成しているがこれに代え、多重鍵で暗号化する方式を採用することもできる。かかる変形例は、同様の仕組みを採用する他の手段についても同様である。
【０１８３】（２）第２のモデル
第２のモデルとして見た下流側システムの復号サーバは、第１の伝送網を通じて配信を受けた部分鍵又はその発生情報と、記録媒体の形態で配信を受けた部分鍵又はその発生情報と、第２の伝送網を通じて配信を受けた合わせ鍵又はその発生情報を基に対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理の解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。
【０１８４】このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する。
【０１８５】（２－２－２）システム構成
本システム例と第１の配信システム例との違いは、合わせ鍵生成部１８で生成された合わせ鍵Ａ１を更に分割する部分鍵生成部２０が追加された点と、当該部分鍵生成部２０で生成された部分鍵を記録媒体に書き込むための書込部２１とその読み取り用の読取部３８が設けられた点と、配信される鍵情報が３つになったことに伴って鍵情報の配信方法に一部変更が生じた点である。
【０１８６】部分鍵生成部２０は、合わせ鍵生成部１８の分割処理により得られた合わせ鍵の一部Ａ１を所定の分割パターンで分割し、一組の部分鍵Ａ１１及びＡ１２を生成する装置である。例えば、配信先となる特定者が１０００人いれば、１０００組の部分鍵Ａ１１及びＡ１２が生成される。もっとも所定の分割パターンはこのように配信先毎に異なる場合だけでなく、全ての配信先について同じでも良い。また、特定地域や管理グループ毎に異なっていても良い。
【０１８７】生成された部分鍵は、部分鍵生成部２０によって配信先管理サーバ１７と所定の配信処理部に与えられる。このシステムの場合、部分鍵生成部２０は、部分鍵Ａ１１をネットワークを介しての配信用に不図示の通信部に与え、残る部分鍵Ａ１２を記録媒体による配信用に書込部２１に与える。
【０１８８】書込部２１は、通知を受けた部分鍵Ａ１２を所定の記録媒体に書き込むための装置である。書込部２１には、記録媒体に応じた駆動機構が設けられる。記録媒体には、磁気読み取り方式の媒体、光学読み取り方式の媒体、半導体メモリその他の媒体が用いられる。なお、記録媒体の配信に必要な宛先情報は配信先管理サーバ１７から与えられる。前述の不図示の通信部についても同様である。ただし、通信部の場合にはネットワーク上のアドレスが与えられる。
【０１８９】なお当該書込部２１と対をなす読取部３８には、配信を受ける記録媒体に応じた駆動機構を備えるものが用いられる。
【０１９０】また、第１の配信システム例では、合わせ鍵生成部１８で生成された合わせ鍵Ａ２は記録媒体を通じて下流側システムに配信されていたが、この第２の配

信システム例の場合、合わせ鍵Ａ２はネットワークを介して配信される。

【０１９１】以上が第２の配信システム例と第１の配信システム例との相違点である。なお基本的なシステム構成については何ら変更がないため、鍵情報の配信動作以外は第１の配信システム例と同様に実行される。

【０１９２】（２－２－３）第２のシステム例によって得られる効果

以上のように第２の配信システム例によれば、鍵情報の配信を２つの伝送網（異なる伝送網を用いる場合と、同一伝送網に異なる時点で鍵情報を配信する場合とがある。）と記録媒体とで実現するため、すなわち第１のシステムよりも更に鍵情報の配信経路が増えるため、伝送経路上での不正行為がより困難なものを提供できる。

【０１９３】（２－３）第３の配信システム例

図６に、上述のビジネスモデルを実現するための第３の配信システム例を示す。ここで図６は、図４及び図５との対応部分に同一符号を付して表したものである。なお第３の配信システム例は前述の第２の手段に対応する。

【０１９４】（２－３－１）概念構成

まず当該第３の配信システム例の概念構成を説明する。この第３の配信システムの場合も、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。

【０１９５】（１）第１のモデル

第１のモデルとして見た上流側システムは、各ディジタルデータに固有の暗号鍵を発生する処理と、ディジタルデータを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、生成された部分鍵の一部又はその発生情報を伝送網を通じて各特定者に配信する処理と、残りの部分鍵又はその発生情報を記録媒体の形態での配信用に鍵専用の第１の記録媒体に書き込む処理と、部分鍵の生成に用いなかった残りの合わせ鍵又はその発生情報を記録媒体の形態での配信用に鍵専用の第２の記録媒体に記録する処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。

【０１９６】一方、下流側システムは、第１の伝送網を通じて配信を受けた部分鍵又はその発生情報と、記録媒体の形態で配信を受けた残りの部分鍵又はその発生情報と、第２の記録媒体の形態で配信を受けた合わせ鍵又はその発生情報を基に対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理とを実行する。

【０１９７】（２）第２のモデル

第２のモデルとして見た下流側システムの復号サーバは、第１の伝送網を通じて配信を受けた部分鍵又はその発生情報と、第２の記録媒体の形態で配信を受けた残りの部分鍵又はその発生情報と、記録媒体の形態で配信を受けた合わせ鍵又はその発生情報を基に対応するディジタルデータに施されている暗号処理を解除する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。

【０１９８】このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する。

【０１９９】（２－３－２）システム構成

本システム例における上流側システムと第２の配信システム例との違いは、合わせ鍵Ａ２の配信がネットワークを介して行われるのではなく、第１の配信システム例のように記録媒体を通じて実現される点である。このため、合わせ鍵Ａ２の配信経路については、第１の配信システム例と同じものが用いられている。

【０２００】以上が第３の配信システムと上述した配信システム例との相違点である。なお基本的なシステム構成については何ら変更がないため、鍵情報の配信動作以外は第１の配信システムや第２の配信システムと同様である。

【０２０１】（２－３－３）第３の配信システム例によって得られる効果

以上のように第３の配信システム例によれば、鍵情報の配信を１つの伝送網と２つの記録媒体とで実現するため、すなわち第２の配信システム例よりも記録媒体による配信経路が増えるため、鍵情報の盗難を発見し易いより不正行為に対する安全性の高いものを提供できる。

【０２０２】（２－４）第４の配信システム例

図７に、上述のビジネスモデルを実現するための第４の配信システム例を示す。ここで図７は、図４との対応部分に同一符号を付して表したものである。なお第４の配信システム例は前述の第１の手段に対応する。

【０２０３】（２－４－１）概念構成

まず当該第４の配信システム例の概念構成を説明する。この第４の配信システムの場合も、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。

【０２０４】（１）第１のモデル
第１のモデルとして見た上流側システムは、各ディジタルデータに固有の暗号鍵を発生する処理と、ディジタルデータを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部を第１の伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵又はその発生情報のうち残りの部分を第２の伝送網を通じて各特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。
【０２０５】一方、下流側システムは、第１の伝送網を通じて配信を受けた合わせ鍵又はその発生情報の一部と、第２の伝送網を通じて配信を受けたそれらと対をなす残りの部分とを基に対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理とを実行する。
【０２０６】（２）第２のモデル
第２のモデルとして見た下流側システムの復号サーバは、第１の伝送網を通じて配信を受けた合わせ鍵又はその発生情報の一部と、第２の伝送網を通じて配信を受けたそれらと対をなす残りの部分とを基に対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理において生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。
【０２０７】このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する。
【０２０８】（２－４－２）システム構成
本システム例における上流側システムと第１の配信システム例との違いは、合わせ鍵生成部１８で発生された合わせ鍵Ａ１及びＡ２がいずれもネットワークを介して配信される点である。
【０２０９】以上が第４の配信システムと第１の配信システム例との相違点である。なお基本的なシステム構成については何ら変更がないため、鍵情報の配信動作以外は第１の配信システム例と同様である。
【０２１０】（２－４－３）第４の配信システム例によって得られる効果
以上のように第４の配信システム例によれば、鍵情報の配信を２つともネットワークを介して実現するため、すなわち全ての鍵情報を即時性に優れたネットワークを通じて配信できるため、記録媒体を使用して鍵情報の配信を行う場合と比べ、鍵の配信からディジタルデータの配信が開始されるまでの時間を大幅に短縮できる。
【０２１１】（２－５）第５の配信システム例
図８に、上述のビジネスモデルを実現するための第５の配信システム例を示す。ここで図８は、図４との対応部分に同一符号を付して表したものである。なお第５の配信システム例は前述の第１の手段に対応する。
【０２１２】（２－５－１）概念構成
まず当該第５の配信システム例の概念構成を説明する。この第５の配信システムの場合も、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。
【０２１３】（１）第１のモデル
第１のモデルとして見た上流側システムは、各ディジタルデータに固有の暗号鍵を発生する処理と、ディジタルデータを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部を記録媒体の形態での配信用に鍵専用の第１の記録媒体に書き込む処理と、生成された合わせ鍵又はその発生情報のうち残りの部分を記録媒体の形態での配信用に鍵専用の第２の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。
【０２１４】一方、下流側システムは、第１の記録媒体の形態で配信を受けた合わせ鍵又はその発生情報の一部と、第２の記録媒体の形態で配信を受けたそれらと対をなす残りの部分とを基に対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を

復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。

【０２１６】このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する。

【０２１７】（２－５－２）システム構成

本システム例における上流側システムと第１の配信システム例との違いは、合わせ鍵生成部１８で発生された合わせ鍵Ａ１及びＡ２がいずれも記録媒体を介して配信される点である。このため、本システムでは、合わせ鍵Ａ１を記録媒体に書き込むための書込部２２と、これと対をなす読取部３９とが新たに設けられている。書込部２２や読取部３９の構成は、他の書込部や読取部の構成と同じである。

【０２１８】以上が第５の配信システム例と第１の配信システム例との相違点である。なお基本的なシステム構成については何ら変更がないため、鍵情報の配信動作以外は第１の配信システムと同様である。

【０２１９】（２－５－３）第５の配信システム例によって得られる効果

以上のように第５の配信システム例によれば、鍵情報の配信を２つとも記録媒体を介して実現するため、すなわち全ての鍵情報を盗難の発見が容易な記録媒体を通じて配信できるため、ネットワークを介して鍵情報を配信する場合と比べ、より不正行為に対する安全性の高いものを提供できる。

【０２２０】（２－６）第６の配信システム例

図９に、上述のビジネスモデルを実現するための第６の配信システム例を示す。ここで図９は、図５との対応部分に同一符号を付して表したものである。なお第６の配信システム例は前述の第２の手段に対応する。

【０２２１】（２－６－１）概念構成

まず当該第６の配信システム例の概念構成を説明する。この第６の配信システムの場合も、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。

【０２２２】（１）第１のモデル

第１のモデルとして見た上流側システムは、各ディジタルデータに固有の暗号鍵を発生する処理と、ディジタルデータを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、生成された部分鍵の一部又はその発生情報を第１の伝送網を通じて各特定者に配信する処理と、残る部分鍵又はその発生情報を第２の伝送網を通じて各特定者に配信する処理と、部分鍵の生成に用いなかった残りの合わせ鍵又はその発生情報を第３の伝送網を通じて各特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。る。

【０２２３】一方、下流側システムは、第１の伝送網を通じて配信を受けた部分鍵又はその発生情報と、第２の伝送網を通じて配信を受けた残りの部分鍵又はその発生情報と、第３の伝送網を通じて配信を受けた合わせ鍵又はその発生情報を基に対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理とを実行する。

【０２２４】（２）第２のモデル

第２のモデルとして見た下流側システムの復号サーバは、第１の伝送網を通じて配信を受けた部分鍵又はその発生情報と、第２の伝送網を通じて配信を受けた残りの部分鍵又はその発生情報と、第３の伝送網を通じて配信を受けた合わせ鍵又はその発生情報を基に対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。

【０２２５】このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する。

【０２２６】（２－６－２）システム構成

本システム例における上流側システムと第２の配信システム例（図５）との違いは、部分鍵生成部２０で発生された部分鍵Ａ１２がネットワークを介して配信される点である。

【０２２７】以上が第６の配信システム例と第２の配信システム例との相違点である。なお基本的なシステム構成については何ら変更がないため、鍵情報の配信動作以外は第２の配信システムと同様である。

【０２２８】（２－６－３）第６の配信システム例によって得られる効果

以上のように第６の配信システム例によれば、鍵情報の

配信を３つともネットワークを介して実現するため、すなわち全ての鍵情報を即時性に優れたネットワークを通じて配信できるため、記録媒体を使用して鍵情報の配信を行う場合と比べ、鍵の配信からディジタルデータの配信が開始されるまでの時間を大幅に短縮できる。

【０２２９】更に、配信される鍵情報の数が３つであるため、２つの鍵情報をネットワークを介して鍵情報を配信する場合と比べ、より不正行為に対する安全性の高いものを提供できる。

【０２３０】（２－７）第７の配信システム例

図１０に、上述のビジネスモデルを実現するための第７の配信システム例を示す。ここで図１０は、図６及び図８との対応部分に同一符号を付して表したものである。なお第７の配信システム例は前述の第２の手段に対応する。

【０２３１】（２－７－１）概念構成

まず当該第７の配信システム例の概念構成を説明する。この第７の配信システムの場合も、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。

【０２３２】（１）第１のモデル

第１のモデルとして見た上流側システムは、各ディジタルデータに固有の暗号鍵を発生する処理と、ディジタルデータを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、生成された部分鍵の一部又はその発生情報を記録媒体の形態での配信用に鍵専用の第１の記録媒体に書き込む処理と、残りの部分鍵又はその発生情報を記録媒体の形態での配信用に鍵専用の第２の記録媒体に書き込む処理と、部分鍵の生成に用いなかった残りの合わせ鍵又はその発生情報を記録媒体の形態での配信用に鍵専用の第３の記録媒体に記録する処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。

【０２３３】一方、下流側システムは、第１の記録媒体の形態で配信を受けた部分鍵又はその発生情報と、第２の記録媒体の形態で配信を受けた残りの部分鍵又はその発生情報と、第３の記録媒体の形態で配信を受けた合わせ鍵又はその発生情報とを基に対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理とを実行する。

【０２３４】（２）第２のモデル

第２のモデルとして見た下流側システムの復号サーバは、第１の記録媒体の形態で配信を受けた部分鍵又はその発生情報と、第２の記録媒体の形態で配信を受けた残りの部分鍵又はその発生情報と、第３の記録媒体の形態で配信を受けた合わせ鍵又はその発生情報とを基に対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。

【０２３５】このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する。

【０２３６】（２－７－２）システム構成

本システム例における上流側システムと第３の配信システム例との違いは、部分鍵生成部２０で発生された部分鍵Ａ１１及びＡ１２がいずれも記録媒体を介して配信される点である。このため、本システム例では、部分鍵Ａ１１を記録媒体に書き込むための書込部２２と、これと対をなす読取部３９とが新たに設けられている。書込部２２や読取部３９の構成は、他の書込部や読取部の構成と同じである。

【０２３７】以上が第７の配信システム例と第３の配信システム例との相違点である。なお基本的なシステム構成については何ら変更がないため、鍵情報の配信動作以外は第３の配信システムと同様である。

【０２３８】（２－７－３）第７の配信システム例によって得られる効果

以上のように第７の配信システム例によれば、鍵情報の配信を３つとも記録媒体を介して実現するため、すなわち全ての鍵情報を盗難の発見が容易な記録媒体を通じて配信できるため、ネットワークを介して鍵情報を配信する経路を含む場合と比べ、より不正行為に対する安全性の高いものを提供できる。

【０２３９】（２－８）第８の配信システム例

図１１に、上述のビジネスモデルを実現するための第８の配信システム例を示す。ここで図１１は、図４との対応部分に同一符号を付して表したものである。当該システム例は、前述までの第１～第７の配信システム例とは異なり、ディジタルデータの暗号鍵を分割するのではなく、当該暗号鍵を配信先毎に固有の別の多重鍵で暗号化するものである。すなわち第８の配信システム例は前述の第３の手段に対応するものである。

【０２４０】（２－８－１）概念構成

まず当該第８の配信システム例の概念構成を説明する。この第８の配信システムの場合も、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。

【０２４１】（１）第１のモデル

第１のモデルとして見た上流側システムは、各ディジタルデータに固有の第１の暗号鍵を発生する処理と、ディジタルデータを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルデータに固有のものを発生する処理と、第２の暗号鍵によって第１の暗号鍵又はその発生情報を暗号化し、伝送網を通じて特定者に配信する処理と、第２の暗号鍵を記録媒体の形態での配信用に鍵専用の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。

【０２４２】一方、下流側システムは、記録媒体の形態で配信を受けた第２の暗号鍵又はその発生情報を基に、伝送網を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除して、対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理とを実行する。

【０２４３】（２）第２のモデル

第２のモデルとして見た下流側システムの復号サーバは、記録媒体の形態で配信を受けた第２の暗号鍵又はその発生情報を基に、伝送網を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除して、対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。

【０２４４】このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する。

【０２４５】（２－８－２）システム構成

前述のように、第８の配信システム例は前述の第１～第７の配信システム例とは基本な処理方式を異にする。このため第８の配信システム例では、配信先に固有の多重鍵Ｂを生成する多重鍵生成部２３と、当該多重鍵Ｂによって暗号鍵Ａを暗号化する鍵暗号化処理部２４と、多重鍵Ｂを記録媒体に書き込んで配信するのに使用する書込部２５と、これと対をなす読取部４０を、第１の配信システム例における合わせ鍵生成部１８、書込部１９、読取部３２に置き換えて使用する。

【０２４６】多重鍵生成部２３は、コンテンツ毎に生成された暗号鍵Ａに配信先毎に固有の暗号鍵Ｂを生成する装置である。例えば、配信先となる特定者が１０００人いれば、１０００通りの多重鍵Ｂを生成する。なお多重鍵Ｂは、配信先が同じであれば常に同じ多重鍵を用いる方法もあれば、コンテンツ毎に異なる多重鍵Ｂを生成して用いる場合もある。安全性の観点からは後者が望ましい。また、特定地域や管理グループ毎に異なる鍵を使っても良い。

【０２４７】鍵暗号化処理部２４は、配信先毎に固有の多重鍵を用いて暗号鍵を暗号化する装置である。鍵暗号化処理部２４で暗号化された暗号鍵は、不図示の通信部よりネットワークを介して対応する下流側システムに配信される。

【０２４８】書込部２５と読取部４０の構成は上述の書込部及び読取部と同じである。もっとも、書込部２５と読取部４０によって読み書きされるのは多重鍵である点で上述の配信システム例とは異なる。

【０２４９】（２－８－３）ディジタルデータの配信動作

第８の配信システム例におけるディジタルデータの配信動作のうち第１の配信システム例と異なる部分についてのみ簡単に説明する。すなわち、第１の配信システム例では、コンテンツに固有の暗号鍵Ａを発生すると当該暗号鍵を合わせ鍵生成部１８に与えて合わせ鍵を生成したが、本システム例の場合、配信先毎に発生された固有の多重鍵Ｂを用いて暗号鍵Ａを暗号化し、ネットワークを介して下流側システムに配信する。また、当該暗号鍵Ａの暗号化に使用した多重鍵Ｂをそれぞれ対応する配信者に宛てて記録媒体の形態で配信する。

【０２５０】なお生成された多重鍵Ｂは、配信先管理サーバ１７にて管理される。以上の処理動作が第１のシステムとの主な違いである。

【０２５１】（２－８－４）第８の配信システム例によって得られる効果

上述のように第８の配信システム例によれば、下流側システムを管理する特定者に配信する鍵情報を暗号化された暗号鍵Ａと多重鍵Ｂとの２つとし、それらを複数の経路を介して配信する構成としたことにより、たとえいずれかの鍵情報が盗難されたとしても他方も盗難されない限り暗号鍵の流出を防止できる配信モデルを提供できる。

【０２５２】しかも多重鍵については盗難を発見し易い

記録媒体の形態で配信を行うため、不正行為によって多重鍵が盗難されたことが明らかにならない場合にはネットワークを介して行う暗号化された暗号鍵Ａの配信を行うのを中止し、別の多重鍵Ｂを記録媒体として配信する手順から再開することで不正行為に対する安全性を保つことができる。

【０２５３】勿論、下流側システムの構成は第１の配信システム例と同じであるため、運用に際しての経済性にも優れることは第１の配信システム例と同様である。

【０２５４】（２－９）第９の配信システム例

図１２に、上述のビジネスモデルを実現するための第９のシステム例を示す。ここで図１２は、図１１との対応部分に同一符号を付して表したものである。なお第９の配信システム例は前述の第４の手段に対応する。

【０２５５】（２－９－１）概念構成

まず当該第９の配信システム例の概念構成を説明する。この第９の配信システムの場合も、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。

【０２５６】第１のモデルとして見た上流側システムは、各ディジタルデータに固有の第１の暗号鍵を発生する処理と、ディジタルデータを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルデータに固有のものを発生する処理と、上記第２の暗号鍵によって第１の暗号鍵又はその発生情報を暗号化し、第１の伝送網を通じて特定者に配信する処理と、第２の暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵の一部又はその発生情報を第２の伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵の残りの部分又はその発生情報を記録媒体の形態での配信用に鍵専用の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。

【０２５７】一方、下流側システムは、第２の伝送網を通じて配信を受けた合わせ鍵の一部と、記録媒体を通じて配信を受けた合わせ鍵の残りの部分とから第２の暗号鍵を復元して、第１の伝送網を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理とを実行する。

【０２５８】（２）第２のモデル

第２のモデルとして見た下流側システムの復号サーバは、第２の伝送網を通じて配信を受けた合わせ鍵の一部と、記録媒体を通じて配信を受けた合わせ鍵の残りの部分とから第２の暗号鍵を復元して、第１の伝送網を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。

【０２５９】このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する。

【０２６０】（２－９－２）システム構成

本システム例と第８の配信システム例との違いは、多重鍵生成部２３で生成された多重鍵Ｂを分割し、一組の合わせ鍵Ｂ１とＢ２を生成する合わせ鍵生成部２６が追加された点と、当該合わせ鍵生成部２６で生成された合わせ鍵の一部Ｂ２を記録媒体に書き込むための書込部２７とその読み取り用の読取部４１が設けられた点である。

【０２６１】合わせ鍵生成部２６は、配信先毎に生成された多重鍵Ｂを配信先毎に固有の分割パターンで分割し、一組の合わせ鍵Ｂ１及びＢ２を生成する装置である。合わせ鍵生成部２６の分割規則は、全ての配信先について共通の分割規則を用いることも可能であるし、配信先毎に固有の分割規則を割り当てることも可能であるし、これら分割規則をコンテンツ単位で変更することも可能である。またコンテンツの配信中も定期又は不定期に変更することも可能である。また特定地域や管理グループ毎に異なる分割規則を割り当てることも可能である。

【０２６２】書込部２７と読取部４１の構成は他の書込部や読取部と同じである。なお基本的なシステム構成については何ら変更がないため、鍵情報の配信動作以外は第８の配信システム例と同様である。

【０２６３】（２－９－３）第９の配信システム例によって得られる効果

以上のように第９の配信システム例によれば、多重鍵Ｂを一組の合わせ鍵Ｂ１及びＢ２に分割して一方をネットワークで、他方を記録媒体で配信する構成を採用するため、すなわち多重鍵Ｂそのものを送るのでなく分割したものを配信するのに加え、配信経路を２つから３つに増やすことにより、第８の配信システム例に比べてより不正行為に対する安全性の高いものを提供できる。

【０２６４】（２－１０）第１０の配信システム例

図１３に、上述のビジネスモデルを実現するための第１０の配信システム例を示す。ここで図１３は、図１２との対応部分に同一符号を付して表したものである。なお第１０の配信システム例は前述の第４の手段に対応する。

【０２６５】（２－１０－１）概念構成

まず当該第１０の配信システム例の概念構成を説明する。この第１０の配信システムには、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。

【０２６６】（１）第１のモデル

第１のモデルとして見た上流側システムは、各ディジタルデータに固有の第１の暗号鍵を発生する処理と、ディジタルデータを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルデータに固有のものを発生する処理と、第２の暗号鍵によって暗号化された第１の暗号鍵又はその発生情報を、記録媒体の形態での配信用に鍵専用の第１の記録媒体に書き込む処理と、第２の暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵の一部又はその発生情報を伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵の残りの部分又はその発生情報を記録媒体の形態での配信用に鍵専用の第２の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。

【０２６７】一方、下流側システムは、伝送網を通じて配信を受けた合わせ鍵の一部と、第２の記録媒体を通じて配信を受けた合わせ鍵の残りの部分とから第２の暗号鍵を復元して、第１の記録媒体を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理とを実行する。

【０２６８】（２）第２のモデル

第２のモデルとして見た下流側システムの復号サーバは、伝送網を通じて配信を受けた合わせ鍵の一部と、第２の記録媒体を通じて配信を受けた合わせ鍵の残りの部分とから第２の暗号鍵を復元して、第１の記録媒体を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先であって、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。

【０２６９】このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する。

【０２７０】（２－１０－２）システム構成

本システム例と第９の配信システム例との違いは、暗号化された暗号鍵Ａの配信をネットワークを介して行うのではなく、記録媒体を介して行う点である。このため、本システム例の場合には、書込部２８と読取部４２が新たに設けられる点で異なっている。書込部２８と読取部４２の構成は他の書込部や読取部と同じであるため省略する。

【０２７１】なお基本的なシステム構成については何ら変更がないため、鍵情報の配信動作以外は第８の配信システム例と同様である。

【０２７２】（２－１０－３）第１０の配信システム例によって得られる効果

以上のように第１０の配信システム例によれば、暗号化された暗号鍵Ａが記録媒体を通じて配信される分、当該鍵がネットワークを介して配信される場合に比して盗難の早期発見が可能となり、暗号鍵の変更等の対策を採り易いという効果を期待できる。

【０２７３】（２－１１）第１１の配信システム例

図１４に、上述のビジネスモデルを実現するための第１１の配信システム例を示す。ここで図１４は、図１１との対応部分に同一符号を付して表したものである。なお第１１の配信システム例は前述の第３の手段に対応する。

【０２７４】（２－１１－１）概念構成

まず当該第１１の配信システム例の概念構成を説明する。この第１１の配信システムには、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。

【０２７５】（１）第１のモデル

第１のモデルとして見た上流側システムは、各ディジタルデータに固有の第１の暗号鍵を発生する処理と、ディジタルデータを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルデータに固有のものを発生する処理と、第２の暗号鍵によって第１の暗号鍵又はその発生情報を暗号化し、第１の伝送網を通じて特定者に配信する処理と、第２の暗号鍵を第２の伝送網を通じて特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。

【０２７６】一方、下流側システムは、第２の伝送網を通じて配信を受けた第２の暗号鍵又はその発生情報を基に、第１の伝送網を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理とを実行する。

【０２７７】（２）第２のモデル

第２のモデルとして見た下流側システムの復号サーバは、第２の伝送網を通じて配信を受けた第２の暗号鍵又はその発生情報を基に、第１の伝送網を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除する処理と、対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。

【０２７８】このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する。

【０２７９】（２－１１－２）システム構成

本システム例と第８の配信システム例との違いは、多重鍵Ｂを記録媒体を介して行うのではなく、ネットワークを介して行う点である。それ以外は第８の配信システム例と同じであるため、鍵情報の配信動作以外は第８の配信システム例と同様である。もっとも、多重鍵Ｂの配信に際しては、電子証明書等で相手方の正当性を確認した上で、配信先が公開している公開鍵で暗号化して配信するのが望ましい。

【０２８０】（２－１１－３）第１１の配信システム例によって得られる効果

以上のように第１１の配信システム例によれば、多重鍵Ｂをネットワークを介して配信する手法を採用するため、鍵の配信からディジタルデータの配信が開始されるまでの時間を大幅に短縮できる。

【０２８１】（２－１２）第１２の配信システム例

図１５に、上述のビジネスモデルを実現するための第１２の配信システム例を示す。ここで図１５は、図１１及び図１３との対応部分に同一符号を付して表したものである。なお第１２の配信システム例は前述の第３の手段に対応する。

【０２８２】（２－１２－１）概念構成

まず当該第１２の配信システム例の概念構成を説明する。この第１２の配信システムには、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。

【０２８３】（１）第１のモデル

第１のモデルとして見た上流側システムは、各ディジタルデータに固有の第１の暗号鍵を発生する処理と、ディジタルデータを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルデータに固有のものを発生する処理と、第２の暗号鍵によって第１の暗号鍵又はその発生情報を暗号化し、記録媒体の形態での配信用に鍵専用の第１の記録媒体に書き込む処理と、第２の暗号鍵を記録媒体の形態での配信用に鍵専用の第２の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。

【０２８４】一方、下流側システムは、第２の記録媒体の形態で配信を受けた第２の暗号鍵又はその発生情報を基に、第１の記録媒体の形態で配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理とを実行する。

【０２８５】（２）第２のモデル

第２のモデルとして見た下流側システムの復号サーバは、第２の記録媒体の形態で配信を受けた第２の暗号鍵又はその発生情報を基に、第１の記録媒体の形態で配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。

【０２８６】このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形

態で出力する処理とを実行する。

【０２８７】（２－１２－２）システム構成

本システム例と第８の配信システム例との違いは、暗号化された暗号鍵Ａの配信をネットワークを介して行うのではなく、記録媒体を介して行う点である。それ以外は第８の配信システム例と同じであるため、鍵情報の配信動作以外は第８の配信システム例と同様である。

【０２８８】（２－１２－３）第１２の配信システム例によって得られる効果

以上のように第１２の配信システム例によれば、鍵情報の配信を２つとも記録媒体を介して実現するため、すなわち全ての鍵情報を盗難の発見が容易な記録媒体を通じて配信できるため、ネットワークを介して鍵情報を配信する場合と比べ、より不正行為に対する安全性の高いものを提供できる。

【０２８９】（２－１３）第１３の配信システム例

図１６に、上述のビジネスモデルを実現するための第１３の配信システム例を示す。ここで図１６は、図１２との対応部分に同一符号を付して表したものである。なお第１３の配信システム例は前述の第４の手段に対応する。

【０２９０】（２－１３－１）概念構成

まず当該第１３の配信システム例の概念構成を説明する。この第１３の配信システムには、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。

【０２９１】（１）第１のモデル

第１のモデルとして見た流側システムは、システム内の何処かに、各ディジタルデータに固有の第１の暗号鍵を発生する処理と、ディジタルデータを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルデータに固有のものを発生する処理と、第２の暗号鍵によって第１の暗号鍵又はその発生情報を暗号化し、第１の伝送網を通じて特定者に配信する処理と、第２の暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵の一部又はその発生情報を第２の伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵の残りの部分又はその発生情報を第３の伝送網を通じて各特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。

【０２９２】一方、下流側システムは、第２の伝送網を通じて配信を受けた合わせ鍵の一部と、第３の伝送網を通じて配信を受けた合わせ鍵の残りの部分とから第２の暗号鍵を復元して、第１の伝送網を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理とを実行する。

【０２９３】（２）第２のモデル

第２のモデルとして見た下流側システムの復号サーバは、第２の伝送網を通じて配信を受けた合わせ鍵の一部と、第３の伝送網を通じて配信を受けた合わせ鍵の残りの部分とから第２の暗号鍵を復元して、第１の伝送網を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルデータに施されている暗号処理を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。

【０２９４】このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する。

【０２９５】（２－１３－２）システム構成

本システム例と第９の配信システム例との違いは、多重鍵Ｂから生成した合わせ鍵Ｂ２の配信に記録媒体を用いるのではなく、ネットワークを介して行う点である。すなわち、３つの鍵情報の配信を全てネットワークを介して行う点で異なっている。それ以外は第９の配信システム例と同じであるため、鍵情報の配信動作以外は第９の配信システム例と同様である。

【０２９６】（２－１３－３）第１３の配信システム例によって得られる効果

以上のように第１３の配信システム例によれば、鍵情報の配信を３つともネットワークを介して行うため、記録媒体を使用して鍵情報の配信を行う場合と比べ、鍵の配信からディジタルデータの配信が開始されるまでの時間を大幅に短縮できる。

【０２９７】更に、配信される鍵情報の数が３つであるため、２つの鍵情報をネットワークを介して鍵情報を配信する場合と比べ、より不正行為に対する安全性の高いものを提供できる。

【０２９８】（２－１４）第１４のシステム例

図１７に、上述のビジネスモデルを実現するための第１４の配信システム例を示す。ここで図１７は、図１３との対応部分に同一符号を付して表したものである。なお第１４の配信システム例は前述の第４の手段に対応す

る。

【０２９９】（２－１４－１）概念構成

まず当該第１４の配信システム例の概念構成を説明する。この第１４の配信システムには、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。

【０３００】（１）第１のモデル

第１のモデルとして見た上流側システムは、各ディジタルデータに固有の第１の暗号鍵を発生する処理と、ディジタルデータを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルデータに固有のものを発生する処理と、第２の暗号鍵によって暗号化された第１の暗号鍵又はその発生情報を、記録媒体の形態での配信用に鍵専用の第１の記録媒体に書き込む処理と、第２の暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵の一部又はその発生情報を記録媒体の形態での配信用に鍵専用の第２の記録媒体に書き込む処理と、生成された合わせ鍵の残りの部分又はその発生情報を記録媒体の形態での配信用に鍵専用の第３の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。

【０３０１】一方、下流側システムは、第２の記録媒体を通じて配信を受けた合わせ鍵の一部と、第３の記録媒体を通じて配信を受けた合わせ鍵の残りの部分とから第２の暗号鍵を復元して、第１の記録媒体を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理とを実行する。

【０３０２】（２）第２のモデル

第２のモデルとして見た下流側システムの復号サーバは、第２の記録媒体を通じて配信を受けた合わせ鍵の一部と、第３の記録媒体を通じて配信を受けた合わせ鍵の残りの部分とから第２の暗号鍵を復元して、第１の記録媒体を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルデータに固有の暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。

【０３０３】このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する。

【０３０４】（２－１４－２）システム構成

本システム例と第１０の配信システム例との違いは、多重鍵Ｂから生成した合わせ鍵Ｂ１の配信にネットワークを用いるのではなく、記録媒体を介して行う点である。すなわち、３つの鍵情報の配信を全て記録媒体を介して行う点で異なっている。このため、本システム例の場合には、書込部２９と読取部４３が新たに設けられている。書込部２９と読取部４３の構成は他の書込部や読取部と同じであるため省略する。

【０３０５】それ以外は第１０の配信システム例と同じであるため、鍵情報の配信動作以外は第１０の配信システム例と同様である。

【０３０６】（２－１４－３）第１４の配信システム例によって得られる効果

以上のように第１４の配信システム例によれば、鍵情報の配信を３つとも記録媒体を介して行うため、すなわち全ての鍵情報を盗難の発見が容易な記録媒体を通じて配信できるため、ネットワークを介して鍵情報を配信する経路を含む場合と比べ、より不正行為に対する安全性の高いものを提供できる。

【０３０７】（３）各システム例で想定される運用形態

第１～第１４の配信システム例では、上流側システムを構成する機能部のいずれが配信権者１のシステム内で行われ、いずれが電子配信事業者２のシステム内で行われるか問題とすることなく（上流側システムが３者以上で運用される場合にはそのいずれかで行われるかを問題とすることなく）、当該システム構成から認められる技術的な効果の観点で説明を行ったが、ここでは想定される運用形態についてビジネス上の効果にどのような差異が生じるかについて説明する。

【０３０８】ここでは特に配給権者から見た上流側システムの安全性について説明する。これは多くの場合、コンテンツの配給権者が不正行為により被害を受けると考えるためであるが、ビジネスモデルによっては他の事業者から見た安全性が優先される可能性があることは言うまでもない。

【０３０９】図１８は、上流側システムを構成する機能部のうち、コンテンツ符号化部１２と、暗号化部１３と、鍵発生部１６（間接的には合わせ鍵生成部（部分鍵生成部）や多重鍵生成部（その合わせ鍵生成部））がどのように配置されるかの観点からまとめたものである。ただし、図１８では、配信される鍵情報が２種類の場合について示されている。３種類以上の鍵情報が配信され

る場合には、図１８に「１つ」と表記された箇所は、「少なくとも１つ」を意味する。

【０３１０】（３－１）第１の運用形態

第１の運用形態では、暗号鍵Ａの発生者、符号化処理の実行者、暗号処理の実行者のいずれもが配給権者である場合（すなわち、コンテンツ符号化部１２、暗号化部１３、鍵発生部１６が配給権者のシステム側に設けられる場合）であって、鍵情報の配信も配給権者が行う場合を考える。

【０３１１】ここで、鍵情報の発生は配給主体である配給権者が行う場合を想定する。すなわち、合わせ鍵生成部１８（システム例によっては部分鍵生成部２０も含む。）や多重鍵生成部２３及び鍵暗号化処理部２４（システム例によっては合わせ鍵生成部２６も含む。）も配給権者が行う場合を想定する。

【０３１２】この場合、電子配信事業者２のシステムは暗号処理の施されたディジタルデータを特定者に配信するだけの業務を行うことになる。すなわち、送出サーバ１４のみが電子配信事業者２のシステムに属することになる。

【０３１３】このような運用形態を採ると、ディジタルデータの暗号化に使用した暗号鍵（マスター鍵）を知り得る立場にある者は配給権者１のみとできる。このことは、配給権者１からみると、電子配信事業者２を通じて暗号鍵が外部に流出する危険性を一切考慮しなくて済むため、安心してコンテンツの提供を行えるという利点がある。

【０３１４】（３－２）第２の運用形態

第２の運用形態では、基本的には第１の運用形態の下に、鍵情報の配信主体が配給権者１と電子配信事業者２の２者となる場合を考える。

【０３１５】例えば、第２の配信システム例（図５）において合わせ鍵Ａ２の生成と配信は配給権者１が行うが、合わせ鍵Ａ１から部分鍵Ａ１１とＡ１２を生成する処理と生成された部分鍵の配信は電子配信事業者２が行う場合が考えられる。この他同様の場合に、第３の配信システム例（図６）、第６の配信システム例（図９）、第７の配信システム例（図１０）が考えられる。

【０３１６】また例えば、生成された合わせ鍵や部分鍵の記録媒体への書込みと配信のみを電子配信事業者２に実行させる場合も考えられる。かかる場合には、第１の配信システム例（図４）、第２の配信システム例（図５）、第３の配信システム例（図６において部分鍵Ａ１２及び又は合わせ鍵Ａ２を書き込む場合）、第５の配信システム例（図８で合わせ鍵Ａ１又はＡ２を書き込む場合）、第７の配信システム例（図１０でいずれか１つの鍵情報又はいずれか２つの鍵情報を書き込む場合）、第９の配信システム例（図１２で合わせ鍵Ｂ２を書き込む場合）、第１０の配信システム例（図１３で暗号化された暗号鍵又は合わせ鍵Ｂ２を書き込む場合）、第１２の配信システム例（図１５で暗号化された暗号鍵を書き込む場合）、第１４の配信システム例（図１７でいずれか１つの鍵情報又はいずれか２つの鍵情報を書き込む場合）がある。

【０３１７】このような運用形態としても、ディジタルデータの暗号化に使用した暗号鍵（マスター鍵）を知り得る立場にある者はコンテンツの配給権者のみとなるため、配給権者にとって安全な運用形態とできる。

【０３１８】なお以上のものに比べるとやや信頼性は低下するが、既存の配信モデルに比して安全性の確保できるものに、第９の配信システム例（図１２）において暗号鍵Ａの暗号化と配信は配給権者１が行うが、多重鍵Ｂの合わせ鍵Ｂ１、Ｂ２の生成と生成された合わせ鍵の配信は電子配信事業者２が行う場合が考えられる。

【０３１９】これと同様のものに第１０の配信システム例（図１３）、第１２の配信システム例（図１５）、第１３の配信システム例（図１６）、第１４の配信システム例（図１７）が考えられる。

【０３２０】（３－３）第３の運用形態

第３の運用形態では、基本的には第１の運用形態の下に、鍵情報の配信主体が電子配信事業者２となる場合を考える。

【０３２１】例えば、第１の配信システム例（図４）において、暗号鍵の発生は配給権者が行うが、発生された暗号鍵を入手して合わせ鍵Ａ１、Ａ２を生成する処理は電子配信事業者２が行う場合が考えられる。これはいずれのシステム例の場合にも考えられる。かかる運用形態を採る場合でも既存の配信モデルに比してシステムの安全性を確保できる。

【０３２２】（３－４）第４～第６の運用形態

これらの運用形態では、第１～第３の運用形態と異なり、暗号化処理を電子配信事業者２が実行する場合を考える。すなわち、電子配信事業者２が暗号鍵を配給権者１から入手して暗号処理を実行する場合である。なお、これらの例では符号化処理は配給権者１側が実行するものとする。

【０３２３】これらの場合では、鍵情報の配信主体が配給権者１のみであるか、電子配信事業者２のみであるか、その両者であるかによらず、結局のところ暗号鍵を知り得る立場にある者がコンテンツ制作会社１と電子配信事業者２の２者となる。ただし、この場合にも既存の配信モデルに比してシステムの安全性を確保できる。

【０３２４】（３－５）第７～第９の運用形態

これらの運用形態では、第４～第６の運用形態に更に加えて、符号化処理の実行も電子配信事業者２が行う場合を考える。これらの運用形態では、配信権者１はもはや暗号鍵を生成しているだけにすぎず、鍵情報の配信主体が配信権者１のみであるか、電子配信事業者２のみであるか、その両者であるかによらず、結局のところ暗号鍵を知り得る立場にある者が配信権者１と電子配信事業者

２の２者となる。ただし、この場合にも既存の配信モデルに比してシステムの安全性を確保できる。

【０３２５】（３－６）第１０～第１２の運用形態

これらの運用形態では、暗号鍵の生成を電子配信事業者２が行って、ディジタルデータの暗号化は電子配信事業者２から暗号鍵の通知を受けた配信権者１が実施する場合を考える。この場合も、鍵情報の配信主体に誰がなるかにかかわらず、結局のところ暗号鍵を知り得る立場にある者は配信権者１と電子配信事業者２の２者となる。ただし、この場合にも既存の配信モデルに比してシステムの安全性を確保できる。

【０３２６】（３－７）第１３～第１８の運用形態

これらのうち第１３～第１５の運用形態は、暗号鍵の生成と暗号化処理を電子配信事業者２が実施し、符号化処理のみを配給権者が行う場合である。また第１６～第１８の運用形態は、暗号鍵の生成、符号化処理、暗号化処理のいずれもを電子配信事業者２が行う場合である。

【０３２７】いずれの運用形態の場合も、鍵情報の配信主体に誰がなるかにかかわらず、結局のところ暗号鍵を知り得る立場にある者は配給権者１と電子配信事業者２の２者となる。なおこの場合も既存の配信モデルに比してシステムの安全性を確保できる。

【０３２８】

【発明の効果】（１）請求項１～５のいずれかに記載の発明によれば、各配信者に固有の複数の鍵情報を発生し、これら複数の鍵情報をディジタルデータとは別の配信経路であって、かつ鍵情報相互においても別の配信経路となるように、すなわち複数の配信経路を用いて個別に配信することにより、暗号鍵を復元するのに必要な全ての情報を一度に入手するのが困難な配信方法を実現できる。また下流側システムを、暗号処理の解除されたディジタルデータにスクランブル処理を施して出力する復号サーバと、当該スクランブル処理を解除する出力装置とで構成することにより、復号サーバと出力装置を結ぶ伝送路上でも不正複製が困難な配信方法を実現できる。

【０３２９】（２）請求項６に記載の発明によれば、下流側システムを、暗号処理の解除されたディジタルデータにスクランブル処理を施して出力する復号サーバと、当該スクランブル処理を解除する出力装置とで構成することにより、復号サーバと出力装置を結ぶ伝送路上でも不正複製が困難な下流側システムを実現できる。

【０３３０】（３）請求項７に記載の発明によれば、その出力信号からはディジタルデータの不正複製が困難な復号サーバを実現できる。また、請求項８に記載の発明によれば、当該回路装置を電子機器に搭載するだけで請求項７の復号サーバと同様の機能を実現できる。また、請求項９に記載の発明によれば、専用装置を用いなくても、請求項７の復号サーバと同様の機能を実現することができる。また、請求項１０に記載の発明によれば、スクランブル制御部と別途組み合わせることで、請求項７の復号サーバと同様の機能を容易に実現可能な復号サーバを実現できる。同様に、請求項１１に記載の発明によれば、当該回路装置とスクランブル制御部とを別途組み合わせて電子機器に搭載するだけで請求項７の復号サーバと同様の機能を実現できる。また、請求項１２に記載の発明によれば、コンピュータをスクランブル制御部として機能させるプログラムと組み合わせることで、専用装置を用いなくても、請求項７の復号サーバと同様の機能を実現できる。同様に、請求項１３に記載の発明によれば、請求項１０に記載の発明と組み合わせることで、請求項７の復号サーバと同様の機能を容易に実現可能な復号サーバを実現できる。同様に、請求項１４に記載の発明によれば当該回路装置と請求項１１に記載の回路装置とを別途組み合わせて電子機器に搭載するだけで請求項７の復号サーバと同様の機能を実現できる。また、請求項１５に記載の発明によれば、請求項１２に記載のプログラムと組み合わせることで、専用装置を用いなくても、請求項７の復号サーバと同様の機能を実現することができる。

【０３３１】（４）請求項１６に記載の発明によれば、その入力信号からはディジタルデータの不正複製が困難な出力装置を実現できる。また、請求項１７に記載の発明によれば、当該回路装置を電子機器に搭載するだけで請求項１６の出力装置と同様の機能を実現できる。また、請求項１８に記載の発明によれば、専用装置を用いなくても、請求項１６の出力装置と同様の機能を実現することができる。

【０３３２】（５）請求項１９に記載の発明によれば、復号サーバが暗号処理の解除されたディジタルデータにスクランブル処理を施して出力する仕組みを採用し、他方、出力装置がディジタルデータに施されているスクランブル処理を解除して所定の出力形態で出力する仕組みを採用することにより、復号サーバと出力装置の伝送路上でも不正複製が困難な下流側システムにおける信号処理方法を実現できる。

【０３３３】（６）請求項２０に記載の発明によれば、復号サーバが暗号処理の解除されたディジタルデータにスクランブル処理を施して出力する仕組みを採用することにより、その出力信号からはディジタルデータの不正複製が困難な復号サーバにおける信号処理方法を実現できる。

【図面の簡単な説明】

【図１】本発明にかかる配信システムの概念を説明する概念構成図である。

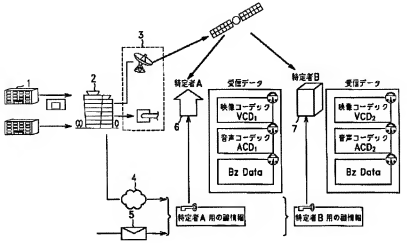
【図２】本発明にかかる配信システムにおける高速配信用ネットワークで配信されるデータのデータ構造を示す図である。

【図３】本発明にかかる配信システムを映画コンテンツに適用した場合について示す図である。

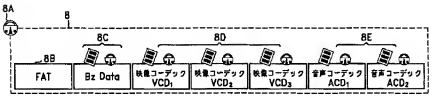
【図４】本発明の実施の形態における第１の配信システ

ムの構成例を示すブロック図である。
【図５】本発明の実施の形態における第２の配信システムの構成例を示すブロック図である。
【図６】本発明の実施の形態における第３の配信システムの構成例を示すブロック図である。
【図７】本発明の実施の形態における第４の配信システムの構成例を示すブロック図である。
【図８】本発明の実施の形態における第５の配信システムの構成例を示すブロック図である。
【図９】本発明の実施の形態における第６の配信システムの構成例を示すブロック図である。
【図１０】本発明の実施の形態における第７の配信システムの構成例を示すブロック図である。
【図１１】本発明の実施の形態における第８の配信システムの構成例を示すブロック図である。
【図１２】本発明の実施の形態における第９の配信システムの構成例を示すブロック図である。
【図１３】本発明の実施の形態における第１０の配信システムの構成例を示すブロック図である。
【図１４】本発明の実施の形態における第１１の配信システムの構成例を示すブロック図である。
【図１５】本発明の実施の形態における第１２の配信システムの構成例を示すブロック図である。
【図１６】本発明の実施の形態における第１３の配信システムの構成例を示すブロック図である。
【図１７】本発明の実施の形態における第１４の配信システムの構成例を示すブロック図である。
【図１８】本発明の実施の形態の構成例として示す各配信システムに共通する運用形態を表示した図である。
【符号の説明】
１　コンテンツサーバ、１２　コンテンツ符号化部、１３　暗号化部、１４送出サーバ、１５　コンテンツ管理サーバ、１６　鍵発生部、１７　配信先管理サーバ、１８，２６　合わせ鍵生成部、１９，２１，２２，２５，２７，２８，２９　書込部、２０　部分鍵生成部、２３　多重鍵生成部、２４　鍵暗号化処理部、３１　受信サーバ、３２，３８，３９，４０，４１，４２，４３　読取部、３３　復号サーバ、３４　出力装置、３４Ａ　デスクランブル部、３５　復号機能部、３５Ａ　復号化部、３５Ｂ　鍵復元部、３５Ｃ　コンテンツ復号化部、３５Ｄ　スクランブル部、３６　スクランブル制御部、３７　出力ログ管理部

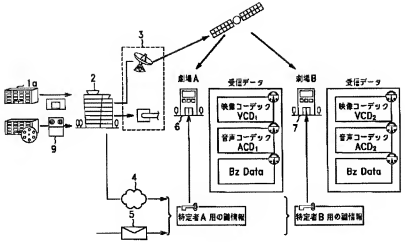
【図１】



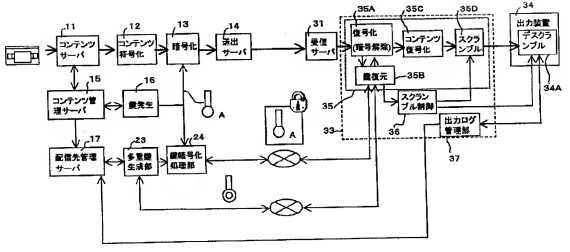

【図２】



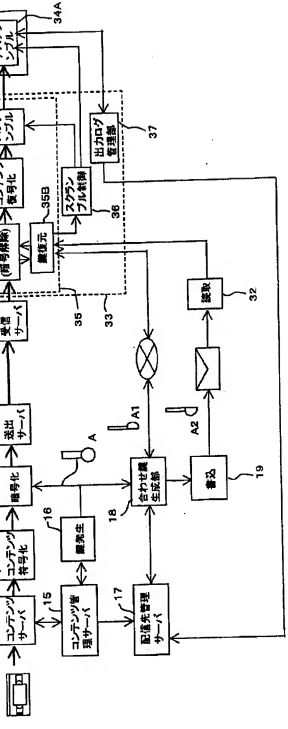
【図３】


劇場A
受信データ
劇場B
受信データ
映像コーデック VCD1
音声コーデック ACD1
Bz Data
映像コーデック VCD2
音声コーデック ACD2
Bz Data
特定者A 用の識情報
特定者B 用の識情報

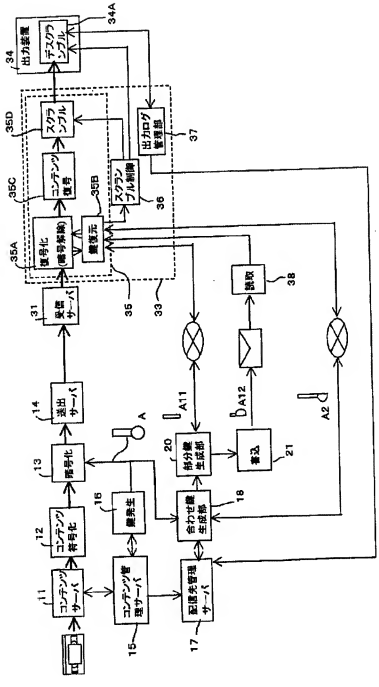
【図１４】


コンテンツサーバ
コンテンツ符号化
暗号化
決出サーバ
受信サーバ
復号化(暗号解除)
コンテンツ復号化
スクランブル
デスクランブル
出力装置
コンテンツ管理サーバ
鍵発生
配信先管理サーバ
多重鍵生成部
鍵暗号化処理部
鍵復元
スクランブル制御
出力ログ管理部

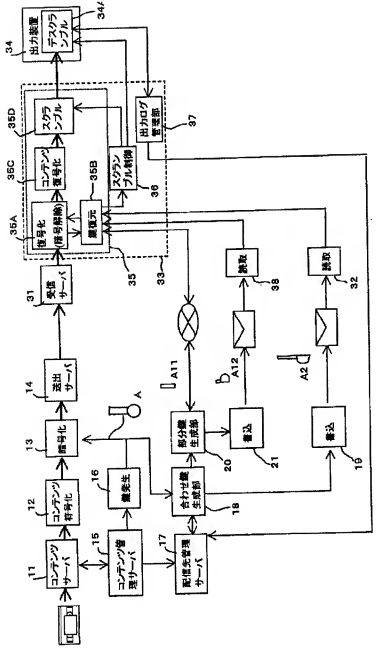
【図4】


11
コンテンツサーバ
12
コンテンツ符号化
13
暗号化
14
送出サーバ
15
コンテンツ管理サーバ
16
鍵発生
17
配信先管理サーバ
18
合わせ鍵生成部
19
書込
A
A1
A2
31
受信サーバ
32
読取
33
35
35A
暗号化(暗号解除)
35B
鍵取得
35C
コンテンツ復号化
35D
スクランブル
34
出力装置
34A
デスクランブル
36
スクランブル制御
37
出力ログ管理部

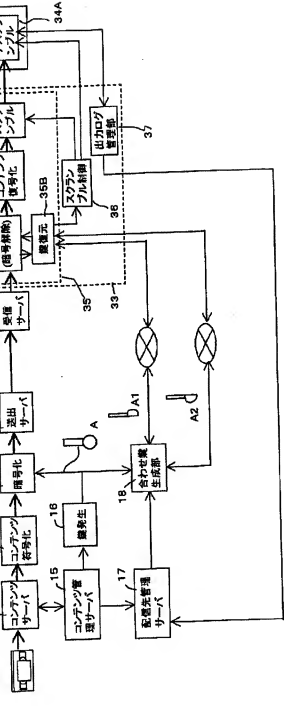
【図５】


11
コンテンツサーバ
12
コンテンツ符号化
13
課金化
14
送出サーバ
31
変調サーバ
35A
復号化（暗号解除）
35B
鍵復元
35C
コンテンツ復号
35D
スクランブル
34
出力装置
34A
デスクランブル
36
スクランブル制御
37
出力ログ管理部
33
35
15
コンテンツ管理サーバ
16
鍵発生
17
利用者管理サーバ
18
合わせ鍵生成部
20
部分鍵生成部
21
蓄積
38
読取
A
A11
A12
A2

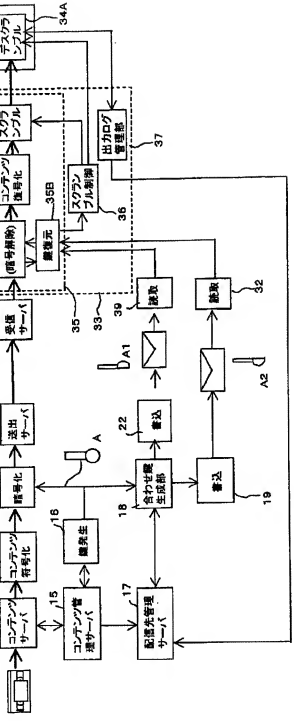
【図６】


11 コンテンツサーバ
12 コンテンツ暗号化
13 暗号化
14 送出サーバ
15 コンテンツ蓄積サーバ
16 鍵発生
17 配信先管理サーバ
18 合わせ鍵生成部
20 部分鍵生成部
21 書込
16 書込
A11
A12
A2
A
31 受信サーバ
32 読取
33
35 復元
35A 復号化（信号解析）
35B スクランブル解除
35C コンテンツ復号化
35D スクランブル
36 出力ログ管理部
37
34 出力装置
34A デスクランブル

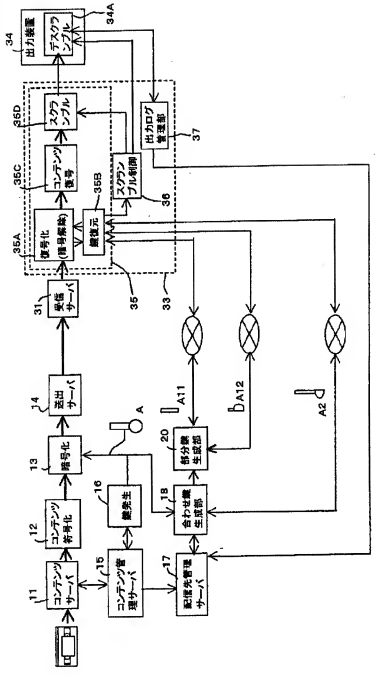
【図７】


11
コンテンツサーバ
12
コンテンツ符号化
13
暗号化
14
蓄出サーバ
15
コンテンツ管理サーバ
16
鍵発生
17
配信先管理サーバ
18
合わせ鍵生成部
A
A1
A2
31
受信サーバ
33
35
35A
復号化（暗号鍵他）
35B
鍵復元
35C
コンテンツ復号化
35D
スクランブル
36
スクランブル制御
37
出力ログ管理部
34
出力装置
34A
デスクランブル

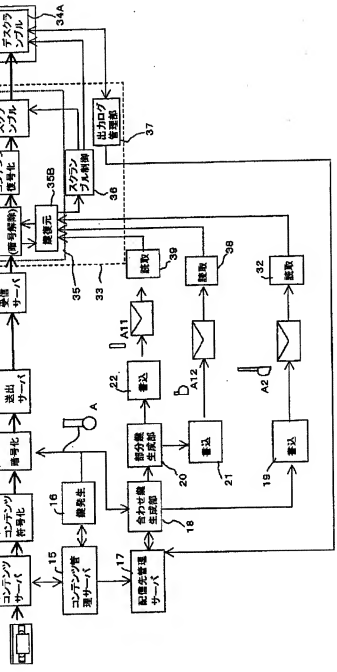
【図８】


11
コンテンツサーバ
12
コンテンツ符号化
13
暗号化
14
送出サーバ
31
受信サーバ
15
コンテンツ管理サーバ
16
鍵発生
17
配信先管理サーバ
18
合わせ鍵生成部
19
書込
A
22
書込
A1
A2
32
読取
39
読取
33
35
35A
暗号化(信号無効)
35B
復号元
35C
コンテンツ復号化
35D
スクランブル
34
出力装置
デスクランブル
34A
スクランブル制御
36
出力ログ管理部
37

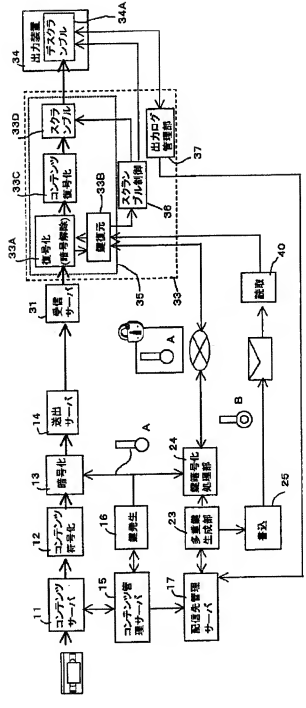
【図９】


34
出力装置
34A
デスクトップ
11
コンテンツサーバ
12
コンテンツ符号化
13
暗号化
14
送出サーバ
31
受信サーバ
35A
復号化
V/A
35B
蓄積元
35C
コンテンツ復号
35D
スクランブル
36
スクランブル制御
37
出力ログ管理部
15
コンテンツ管理サーバ
16
鍵発生
17
配信先管理サーバ
18
合わせ鍵生成部
20
部分鍵生成部
A
A11
A12
A2
33
35

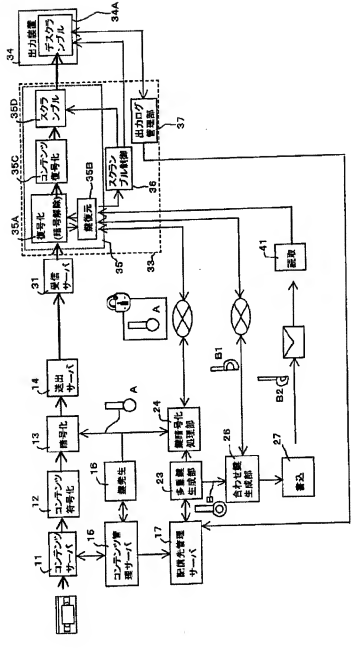
【図１０】


11
コンテンツサーバ
12
コンテンツ符号化
13
暗号化
14
送出サーバ
15
コンテンツ管理サーバ
16
鍵発生
17
配信先管理サーバ
18
合わせ鍵生成部
19
書込
20
部分鍵生成部
21
書込
22
書込
A
A11
A12
A2
31
受信サーバ
32
読取
33
35
35A
復号化（暗号解除）
35B
鍵選択
35C
コンテンツ復号化
35D
スクランブル
36
スクランブル解除
37
出力ログ管理部
34
出力装置
34A
デスクランブル
39
読取
38
読取

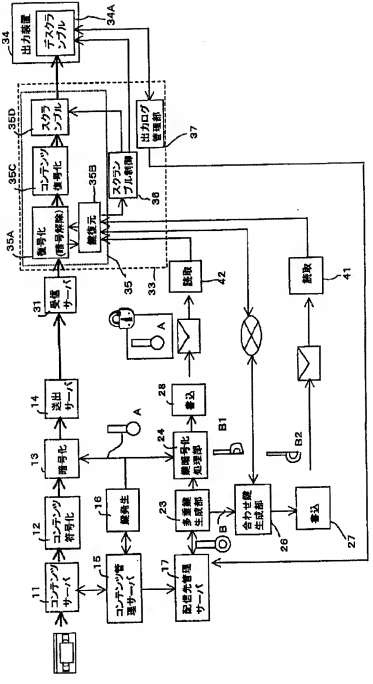
【図１１】


11
コンテンツサーバ
12
コンテンツ符号化
13
識別符号化
14
送出サーバ
15
コンテンツ管理サーバ
16
鍵発生
17
知識免管理サーバ
23
多重鍵生成部
24
識別符号化処理部
25
書込
31
受信サーバ
32A
復号化（暗号解読）
33
鍵保存
33B
スクランブル制御
33C
コンテンツ復号化
33D
スクランブル
34
出力装置
34A
デスクランブル
35
36
37
出力ログ管理部
40
読取
A
B

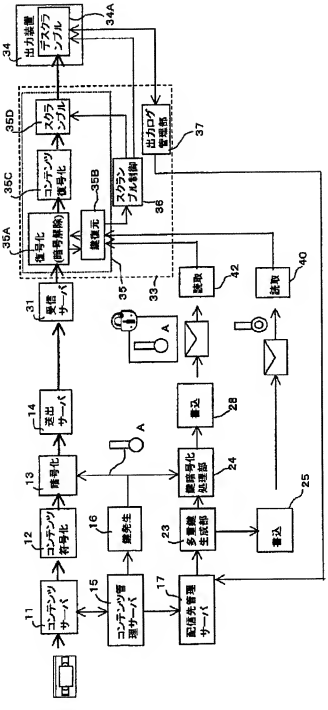
【図１２】


34
出力装置
34A
ディスプレイ
35
35D
スクランブル
35C
コンテンツ復号化
35B
スクランブル制御
35A
復号化（信号解析）
復元
36
37
出力Ｄ／Ａ変換装置
33
31
受信サーバ
41
蓄積
14
送出サーバ
13
符号化
24
課題学化処理部
26
合わせ編集処理部
27
書込
B1
B2
12
コンテンツ符号化
16
編集生
23
生編集処理部
11
コンテンツサーバ
16
コンテンツ管理サーバ
17
配信先管理サーバ

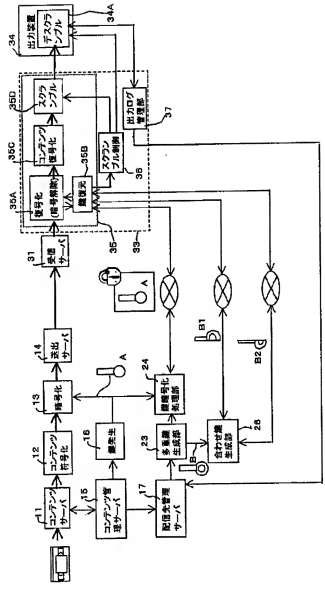
【図１３】


34
出力装置
34A
デスクトップル
35D
スクランブル
35C
コンテンツ復号化
35B
スクランブル制御
35A
復号化
信号解読
鍵保元
36
37
出力ログ管理部
31
受信サーバ
35
33
課金
42
41
課税
A
B1
B2
28
書込
14
送出サーバ
13
暗号化
24
暗号化処理部
12
コンテンツ符号化
16
鍵発生
23
多重暗号生成部
26
合わせ鍵生成部
27
書込
11
コンテンツサーバ
15
コンテンツ管理サーバ
17
配信先管理サーバ
B

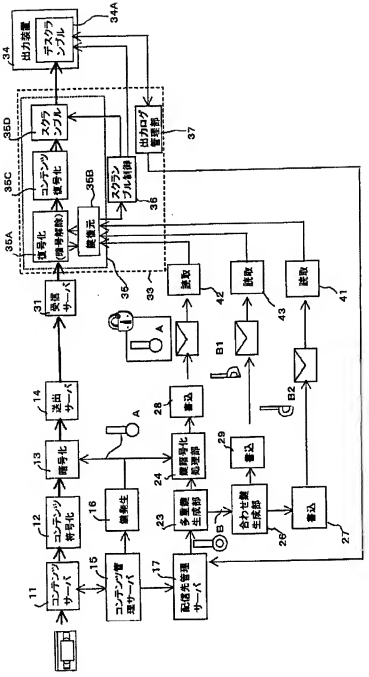
【図１５】


11
コンテンツサーバ
12
コンテンツ符号化
13
鍵符号化
14
配出サーバ
15
コンテンツ管理サーバ
16
鍵発生
17
配信先管理サーバ
23
多重鍵生成部
24
鍵符号化処理部
25
書込
28
書込
31
実標サーバ
33
35
35A
復号化（鍵符号解除）
35B
鍵復元
35C
コンテンツ復号化
35D
スクランブル
36
スクランブル制御
37
出力ログ管理部
34
出力装置
デスクランブル
34A
読取
42
読取
40
A
A

【図１６】


11 コンテンツサーバ
12 コンテンツ符号化
13 暗号化
14 送出サーバ
15
16 鍵生成
17 配信先管理サーバ
18 コンテンツ管理サーバ
21 鍵暗号化処理部
22 鍵情報生成部
23 鍵情報生成部
24
25 合わせ鍵生成部
31 受信サーバ
32 復号化
33 暗号解除
34 出力装置
34A デスクランブル
35 VOD管理部
35A
35B
35C コンテンツ符号化
35D スクランブル
36 スクランブル制御
37 出力ログ管理部
38 課金処理
A
B1
B2

【図１７】


11
コンテンツサーバ
12
コンテンツ符号化
13
暗号化
14
出荷サーバ
15
コンテンツ管理サーバ
16
鍵発生
17
配信先管理サーバ
23
多重鍵生成部
24
鍵情報暗号処理部
26
合わせ鍵生成部
27
書込
28
書込
29
書込
31
発注サーバ
33
35
35A
改竄化（電子透かし）
35B
改竄検出
35C
コンテンツ復号化
35D
スクランブル
34
出力装置
34A
デスクランブル
36
スクランブル制御
37
出力ログ管理部
41
読取
42
読取
43
読取
A
B
B1
B2

【図１８】

| | 暗号鍵の発生者 | 符号化実行者 | 暗号化実行者 | 鍵情報の配信者 | 配給複者から見たシステムの安全性 | 備考 |
|---|---|---|---|---|---|---|
| 1 | 制作者 | 制作者 | 制作者 | 制作者(2つ) | ＋＋＋ | |
| 2 | 同上 | 同上 | 同上 | 制作者(1つ)＋配信者(1つ) | ＋＋ | 配信者が暗号化された暗号鍵を入手 |
| 3 | 同上 | 同上 | 同上 | 配信者(2つ) | ＋＋ | 配信者が暗号鍵を入手して鍵情報を作成 |
| 4 | 同上 | 同上 | 配信者 | 制作者(2つ) | ＋＋ | 暗号鍵は配信者に通知される |
| 5 | 同上 | 同上 | 同上 | 制作者(1つ)＋配信者(1つ) | ＋＋ | 同上 |
| 6 | 同上 | 同上 | 同上 | 配信者(2つ) | ＋＋ | 同上 |
| 7 | 同上 | 配信者 | 同上 | 制作者(2つ) | ＋＋ | 同上 |
| 8 | 同上 | 同上 | 同上 | 制作者(1つ)＋配信者(1つ) | ＋＋ | 同上 |
| 9 | 同上 | 同上 | 同上 | 配信者(2つ) | ＋＋ | 同上 |
| 10 | 配信者 | 制作者 | 制作者 | 制作者(2つ) | ＋ | 制作者が暗号鍵を入手して鍵情報を作成 |
| 11 | 同上 | 同上 | 同上 | 制作者(1つ)＋配信者(1つ) | ＋ | 同上 |
| 12 | 同上 | 同上 | 同上 | 配信者(2つ) | ＋ | 同上 |
| 13 | 同上 | 同上 | 配信者 | 制作者(2つ) | ＋ | 同上 |
| 14 | 同上 | 同上 | 同上 | 制作者(1つ)＋配信者(1つ) | ＋ | 同上 |
| 15 | 同上 | 同上 | 同上 | 配信者(2つ) | ＋ | 同上 |
| 16 | 同上 | 配信者 | 同上 | 制作者(2つ) | ＋ | 同上 |
| 17 | 同上 | 同上 | 同上 | 制作者(1つ)＋配信者(1つ) | ＋ | 同上 |
| 18 | 同上 | 同上 | 同上 | 配信者(2つ) | ＋ | 同上 |